VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Technologie počítačových sítí pro podporu Cloud Computingu

Computer Network Technologies for Cloud Computing

2013 **Bc. Lukáš Adamčík**

VŠB - Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Zadání diplomové práce

Student: **Bc. Lukáš Adamčík**

Studijní program: N2647 Informační a komunikační technologie

Studijní obor: 2612T025 Informatika a výpočetní technika

Téma: Technologie počítačových sítí pro podporu cloud computingu
Computer Network Technologies for Cloud Computing

Zásady pro vypracování:

1. Proveďte rešerši současných definic a pojetí cloud computingu.
2. Prozkoumejte současné technologie implementace a řízení provozu virtualizovaných strojů provozovaných v rámci cloud computingu.
3. Sumarizujte typické požadavky cloud computingu na síťovou infrastrukturu se zohledněním mobility virtuáních strojů. Popište současné techniky pro udržení nastavení přístupových portů jednotlivých migrujících VM.
4. Prozkoumejte možnosti implementací virtuálních síťových prvků v nejpoužívanějších hostitelských platformách (i řešení distribuovaná přes více hostitelských serverů). Popište možnosti jejich komunikace s fyzickými síťovými prvky a způsoby podpory servisních L2 protokolů (STP, LACP, LLDP, ...).
5. Realizujte a zdokumentujte případové studie demonstrující možnosti virtualizovaných přepínačů. Zaměřte se zejména na VMWare ESX server a Cisco Nexus 1000V.

Seznam doporučené odborné literatury:

[1] Jamsa, K.: Cloud Computing. Jones & Bartlett Learning, Burlington 2012, ISBN 1449647391.
[2] Josyula, V., Ott, M., Page, G.: Cloud Computing: Automating the Virtualized Data Center. Cisco Press, Indianapolis, 2011, ISBN 1587204347.

Formální náležitosti a rozsah diplomové práce stanoví pokyny pro vypracování zveřejněné na webových stránkách fakulty.

Vedoucí diplomové práce: **Ing. Petr Grygárek, Ph.D.**

Datum zadání: 16.11.2012
Datum odevzdání: 07.05.2013

doc. Dr. Ing. Eduard Sojka
vedoucí katedry

prof. RNDr. Václav Snášel, CSc.
děkan fakulty

Prohlášení studenta

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně. Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

Dne: *7.5.2013*

.....

Poděkování

Rád bych poděkoval panu Ing. Petru Grygárkovi, Ph.D. za odbornou pomoc a konzultaci při vytváření této diplomové práce.

Abstrakt

Tato práce pojednává o cloud computing - rozebírá možnosti současných řešení cloud a možnosti implementací cloud od jednotlivých společností. Analyzuje vlastnosti jednotlivých virtuálních přepínačů, jako jsou vSwitch, Virtual Distributed Switch a Cisco NEXUS 1000v. Probírá současnou funkcionalitu virtualizací od firem VMware, Microsoft, IBM a také testuje možnosti VXLAN v rámci síťové infrastruktury ve spojení se směrovači Cisco. Prozkoumává možnosti vytvoření vlastního private cloud v rámci jednoduché síťové infrastruktury a virtualizace od společnosti VMware.

Klíčová slova

cloud computing, VMware, System center, VLAN, VXLAN, vSphere, private cloud, veřejný cloud, virtuální přepínač, vCenter, vSphere, ESXi

Abstract

This Master's Thesis deals with a Cloud Computing – it analyses possibilities of current cloud solutions and options of cloud implementations of particular firms. It further analyses network operation and properties of individual virtual switches such as vSwitch, vSphere Distributed Switch a Cisco NEXUS 1000v. It tests possibilities of settings preservation on the ports during migration of virtual PCs on Cisco NEXUS 1000v switch. It describes current functionality of virtualizations of VMware, Microsoft, IBM and also tests possibilities of WXLAN within the network infrastructure in connection with Cisco routers. The thesis investigates options of creating own private cloud within a simple network infrastructure.

Key words

cloud computing, VMware, System center, VLAN, VXLAN, vSphere, private cloud, public cloud, virtual swich, vCenter, vSphere, ESXi

Seznam použitých zkratek

Zkratka	Anglický význam	Vysvětlení
CDP	Cisco Discovery Protocol	Cisco protokol sloužící k propagaci identity do síťě
HA	High Availability	Automatizované řešení ochrany proti selhání fyzického hardware
LACP	Link Aggregation Control Protocol	Protokol kontrolující nastavení agregace linky
LLDP	Link Layer Discovery Protocol	Protokol sloužící k propagaci identity do síťě
NIC	Network interface controller	Fyzický síťový adaptér
PG	Port-group	Je to skupina portů, pro kterou platí stejná konfigurace
SC	System Center	Systémové centrum
STP	Spanning Tree Protocol	STP se používá, aby nedocházelo ke smyčkám v síti
VDS/dvSwitch	Virtual Distributed Switch	Virtuální distribuovaný přepínač
VM	Virtual machine	Virtuální PC
VNI	VXLAN Network Identifier	Indentifikátor určité VXLAN
vSwitch	Virtual Swtich	Virtuální přepínač

Obsah

1 Úvod

V dnešní době se rozmáhá a také se hodně mluví o takzvaném cloud computing, jehož technologiemi se bude tato práce zabývat. Cloud computing je nový model konzumace (využívání) a poskytování IT služeb s využitím Internetových technologií. Představuje nové evoluční paradigma v oblasti konsolidace, virtualizace a poskytování IT služeb s tím, že virtualizace je základním katalyzátorem technologie cloud computing. Uživatelé mají možnost přistupovat ke svým údajům pomocí internetového prohlížeče nebo speciálního klienta pro aplikaci. Přistoupit mohou z jakéhokoli počítače. Některé služby v cloud computing jsou zadarmo, některé se musí platit. V cloud computing (zkráceně CC) jsou pro uživatele k dispozici systémy pro distribuované výpočty a také operační systémy, běžící v prohlížečích. V neposlední řadě je možné provozovat také virtuální aplikace. Tato práce se bude zabývat především virtuálními PC a virtuálními přepínači.

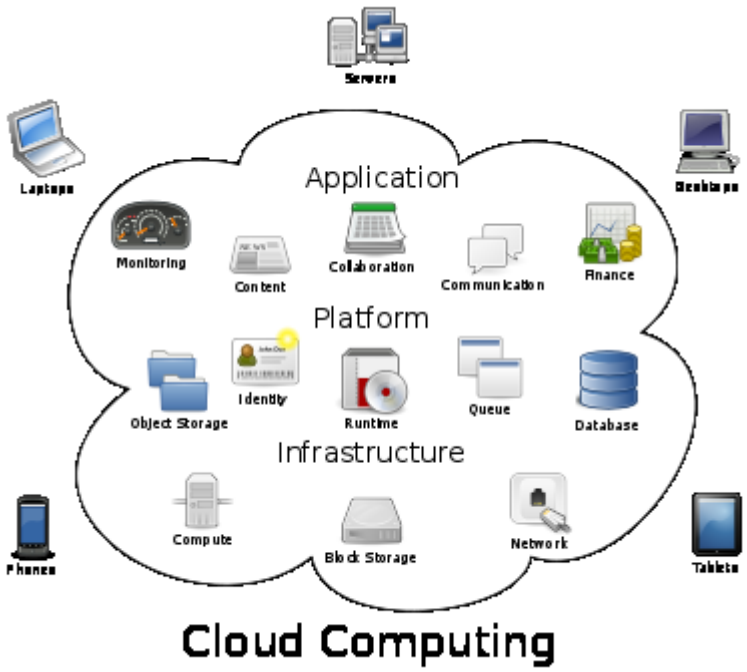
V dnešní době poskytuje cloud computing mnoho společností. V mé práci jsem si vybral tři velké společnosti, jejichž cloud systémy prozkoumám. Jednou je IBM, druhou VMWARE a třetí je Microsoft. Pro svou studii využiji VMware cloud, který se mi jeví jako nejvíce rozšířený a dobře dostupný. Práce rozebere cloud vlastnosti jednotlivých společností – výhody, nevýhody atd.

Ve své analýze cloud computing, jak jsem již zmínil, se budu zabývat virtuálními přepínači a virtuálními PC, připojenými k těmto přepínačům. Budu testovat jejich vlastnosti v rámci síťové infrastruktury. Dále budu sledovat, zda jsou přepínače schopny, při migraci virtuálního PC, si zapamatovat nastavení pro port, ke kterému je virtuální PC připojeno. Budu testovat a zkoumat jednotlivé nastavení přepínačů a následné vlivy na virtuální síť a počítače komunikující v této síti. Také si otestuji virtuální přepínač NEXUS 1000v.

V neposlední řadě budu testovat aplikační část cloudu, tedy využívání koncových aplikací uživateli, např. funkčnost, rychlost, výhody, nevýhody.

2 Cloud computing

Pro lepší znázornění a uvědomění si „co je cloud“, bych na začátek zvolil jako ilustraci obrázek 2.1. Tento obrázek charakterizuje vše, co je cloud computing schopný poskytnout a jakých oblastí ve světě Informační technologie se vlastně týká. Obrázek 2.1 také zobrazuje technologie, jakými cloud oplývá. Tedy zakládá se na stabilní infrastruktuře, kterou tvoří fyzické servery. Na těchto serverech běží software, který vytváří prostředí pro jednotlivá odvětví cloud computing. Jsou to různé aplikace, které lze využívat odkudkoliv z prostředí internetu a také na různých platformách [1]. Dále je možné tvořit virtuální počítače s operačními systémy Widnows, Linux a s mnoha dalšími (Apple Mac OS, IBM OS/2, Sun Microsystems Solaris), které lze poté vzdáleně spravovat a provádět na nich úkony jako na normálním fyzickém PC. Ve virtuálním prostředí lze používat graficky náročné programy jako jsou CAD systémy atd. Pro tyto programy je ovšem nutné přizpůsobit hardware dané infrastruktury. Po hardwarovém přizpůsobení infrastruktury, lze na těchto virtuálních PC také provádět grafické operace. Prostředí cloud computing je hojně využíváno i pro testovací a vývojové účely.



Obrázek 2.1 - „Cloud Computing“ [2]

V této kapitole bych se chtěl zaměřit na rozdělení cloud podle řešení, na kterých jsou postaveny - VMware, MICROSOFT a IBM. V další kapitole bych pak uvedl varianty, které poskytují jednotlivé firmy na bázi řešení od společností VMware, MICROSOFT a IBM. Kromě popisů

jednotlivých variant nabízených služeb jednotlivými společnostmi, se budu zabývat podstatou těchto nabízených služeb.

2.1 IBM Cloud

Začnu tedy s popisem IBM Cloud. Ten rozděluje svoji službu na private cloud a public cloud, s tím, že se public cloud ještě dělí na IBM Smart Business Desktop on the IBM Cloud a IBM SmartCloud Enterprise. Tyto produkty jsou vhodné jak pro malé a střední firmy, tak pro větší korporace.

Cloud od IBM jsem měl možnost si vyzkoušet v testovací verzi. V této verzi si lze přes webové rozhraní vytvořit virtuální server s operačním systémem Linux a uvést ho do provozu. Bohužel práce s virtuálními PC už není v testovací verzi možná. Toto řešení se u IBM nazývá SmartCloud Enteprise. Také jsem měl možnost vidět řešení private cloud. Na první pohled jsem rozpoznal, že se jedná o webové rozhraní poskytované produktem vCloud od společností VMware. Jak jsem ale později zjistil, private cloud od IBM obsahuje ještě navíc software, který se stará o správu celého private cloud [3].

2.2 VMware Cloud

Společnost VMware, která zaujímá vedoucí postavení v oblasti virtualizace, dokáže provozovat na svých cloud systémech robustní aplikace a také je schopna dodávat výpočetní prostředí pro koncové uživatele. VMware rozděluje cloud službu na private cloud, public cloud a hybrid cloud. Zvláštností je zde hybrid cloud, který kombinuje služby private a public cloud dohromady. Se společností VMware je možné uzavřít partnerství, o poskytování cloud služeb s řešením od VMware. Partneři společnosti VMware poté poskytují klientům svá datacentra pro provoz cloud systémů. Takovýmto partnerem je například společnost O2, s produktem O2 Cloud, který je popsán v dalších kapitolách. Taková partnerství uzavírají i společnosti IBM a Microsoft.

Virtuální prostředí od VMware jsem měl možnost si vyzkoušet. Software od VMware mě zaujal nejen svým rozhraním, ale i docela snadným vytvořením virtuálních PC. Také je velmi zajímavá migrace virtuálních PC mezi jednotlivými ESXi PC, například při výpadku. Těmito a dalšími nástroji je mocný VMware vybaven, a proto jsem si ho vybral pro své testování [4].

2.3 Microsoft Cloud

Na závěr jsem si nechal popis Microsoft Cloud. U tohoto cloud jsem narazil na výjimku oproti ostatním cloud systémům. Proti IBM má Microsoft postavený private cloud na vlastním řešení.

Microsoft rozděluje svoji cloud službu na private cloud a public cloud. Také, stejně jako VMware, nabízí partnerství pro poskytovatele Microsoft služeb.

Na Microsoft stránkách je možné po registraci si private cloud stáhnout, nainstalovat a vyzkoušet, což jsem také učinil. Produkt, pod kterým je private cloud provozován se jmenuje SYSTEM CENTER. Tento produkt je založen na systému Hyper-V a Windows Server. Public cloud je založený na webové platformě jménem Windows Azure, pomocí které mohou klienti svůj cloud spravovat [5].

3 Varianty jednotlivých Cloud řešení

3.1 Varianty řešení od IBM

3.1.1 Private cloud - řešení Entry Cloud

Private cloud je řešení, u něhož IBM nabízí variantu Entry Cloud. Toto řešení je dodávka cloud řešení typu **IaaS** (Infrastructure as a Service), což je jedním z nejrychleji nasaditelných řešení cloud typu pro IX-86 platformu (Linux/Windows). Jedná se tedy o dodávku hardware, cloud software a služeb pro implementační fázi. Toto řešení je vhodné pro větší korporace, které si chtějí založit svůj vlastní cloud. Řešení od IBM obsahuje konfiguraci s VMware platformou, na které lze vytvořit několik desítek virtuálních PC s libovolným operačním systémem, který VMware podporuje. Počet virtuálních PC je omezen pouze hardware konfigurací ESXi serverů.

Současně s hardware a VMware software je součástí dodávky produkt IBM Service Delivery Manager, což je platforma pro správu cloud systémů. Ta datovému centru umožňuje urychlit vytváření platforem služeb pro široké spektrum typů pracovních zátěží s vysokým stupněm integrace, flexibility a optimalizace prostředků s těmito hlavními funkcemi pro správu služeb. Předem integrovaná sada software je poskytována jako balíček virtuálních obrazů, které je možno vypálit na cd/dvd. Nasazení této varianty je otázkou několika týdnů [6].

3.1.2 IBM Public Cloud

Public cloud může nabídnout různé služby (např. Smart Business Desktop), které jsou zaměřeny na provoz aplikací, uchování informací a jsou přístupné odkudkoliv z internetu. Dále také poskytuje služby jako například SmartCloud Enterprise, což je prostředí určené pro bezpečný vývoj aplikací. Public cloud nabízí virtualizaci i od jiných společností než VMware. Virtualizace lze zde využít i od firem Citrix, Wyse a Virtual Bridges.

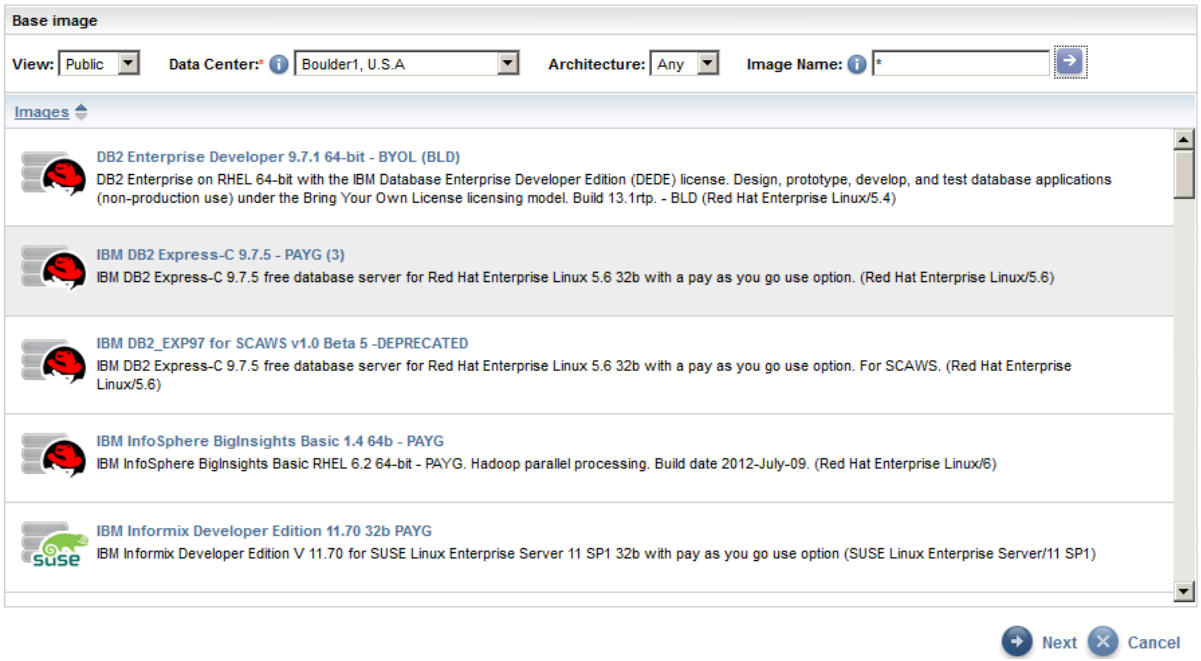
3.1.2.1 IBM SmartCloud Enterprise

Toto prostředí slouží převážně pro vývoj a testování aplikací pomocí připraveného bezpečného vývojového prostředí na IBM Cloud. Tato infrastruktura jako servisní řešení (IaaS) přispívá ke kratší době vývojových a testovacích cyklů. Klient při ladění získává okamžitě přístup k požadované infrastruktuře prostřednictvím Internetu a může začít pracovat. Toto řešení je k dispozici v prostředí datových center IBM. Výhody jsou podobné jako u předchozí varianty - úspora peněz za hardware a správa infrastruktury.

Tento IBM Smart Cloud je možné si vyzkoušet na internetu, což jsem také učinil. Prostředí je jiné než u private cloud od VMware. Pro tento cloud má firma IBM vyvinuto vlastní prostředí. V testovací verzi lze vyzkoušet například tyto cloud platformy:

- PureSystems™ patterns
- DB2®
- Informix®
- BigInsights™

Obrázek 3.1 ilustruje různé typy platforem a jejich výběr při vytváření nového virtuálního PC.

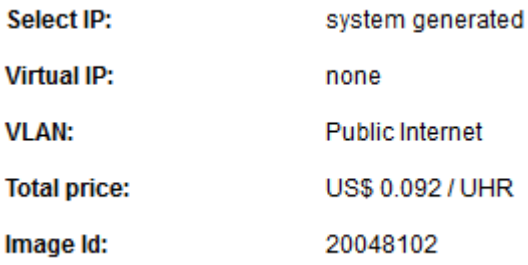


Obrázek 3.1 - „prostředí IBM Smart Cloud“ [30]

Dále lze při výběru platformy specifikovat vlastnosti této platformy, jak ukazuje obrázek 3.2.

Obrázek 3.2 - „Vlastnosti platformy v IBM Smart Cloud prostředí“ [30]

V konečném soupisu lze vidět i částku, jakou bude pronajímaná platforma stát – viz. obrázek 3.3.

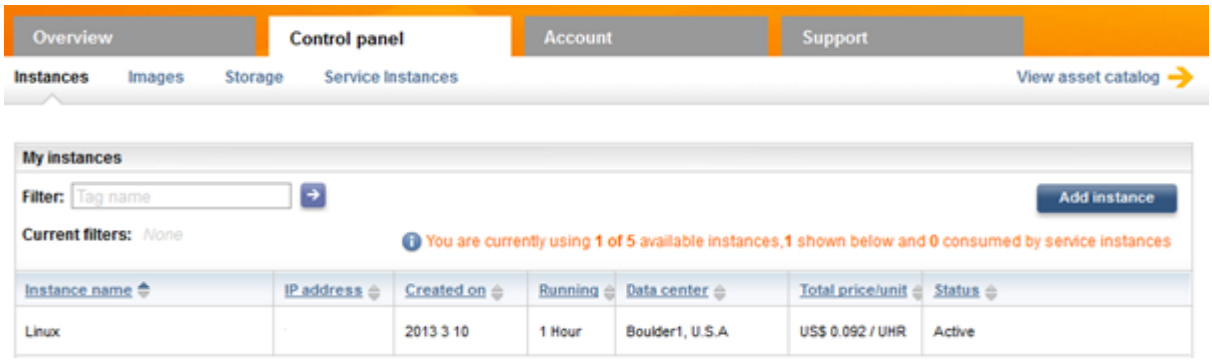


Obrázek 3.3 - „Konečný soupis najímané platformy“ [30]

Na těchto platformách je možné vyvíjet, testovat a rychle nasazovat aplikace do cloud za minimálními finanční prostředky, než které bychom zaplatili při zřízení reálného fyzického serveru. Využití pro firmy bych viděl v tom, že tímto nasazováním aplikací na stejné platformě jako na vývojové, se urychlí doby cyklu, sníží se počet chyb a náklady. V tomto zkušebním prostředí je možné si vyzkoušet až 5 virtuálních PC [7].

Na obrázku 3.4 je vidět soupis použitých virtuálních PC. V mém případě jde o jedno virtuální PC, na které se přistupuje pomocí veřejné IP adresy.

.



Obrázek 3.4 - „Soupis použitých virtuálních PC“ [30]

3.1.2.2 IBM Smart Business Desktop on the IBM

Je řešení, které poskytuje kdykoliv a kdekoliv přístup k aplikacím, informacím a prostředkům. Jedná se tedy o spolehlivé a bezpečné počítačové prostředí, provozované v datovém centru IBM na IBM Cloud.

Výhody tohoto nasazení plynou hlavně z toho, že se používají pouze koncová zařízení, kterými se aplikace z cloud spravují. Veškeré výpočetní prostředí je tedy centralizováno – existuje centrální správa – standardní katalog se standardně používaným softwarem.

3.1.3 Rozdíl mezi Public a Private Cloud

Private cloud je určen pro menší firmy a organizace, kde je dodáván kompletní hardware i se software od VMware. Tento cloud je dostupný pouze z prostředí cílové firmy. Oproti tomu public cloud je dosažitelný odkudkoliv z internetu, tedy jeho uživatelé mohou přistupovat ke svým zdrojům odkudkoliv, kde mají připojení k internetu. Tento cloud je poskytován jako služba převážně pro větší firmy. Hardware je poskytován v rámci služby firmou IBM, tedy z jejich datových center a v rámci public cloudu nabízí IBM virtualizaci i od jiných společností než VMware, Citrix, Wyse a Virtual Bridges.

3.2 Varianty řešení od VMWARE

3.2.1 VMware Private Cloud

Private cloud je určen pro zvýšení výkonnosti, stability a bezpečnosti datového centra kontrolovaného pomocí software od VMware. Toto řešení slouží pro sjednocení stávajících datových center, a s využitím jejich celkové výkonnosti pro provoz virtuálních PC v rámci celé infrastruktury. U private cloud lze definovat také takzvané role, které zabezpečí, aby se uživatelé dostali jen na přidělené virtuální PC, které mohou spravovat. Tato varianta cloud systému je vhodná pro menší a střední firmy [8].

3.2.2 VMware Public & Hybrid Cloud Computing

Toto řešení je vhodné, pokud je potřeba dodatečně navýšit kapacity virtualizované infrastruktury nebo pokud je potřeba nahradit velké datové centrum za virtualizovanou infrastrukturu. V této variantě je možno zkombinovat možnosti public a private cloud, tedy posílit stávající virtuální infrasktrukturu private cloud pomocí výkonu z public cloud. Tohoto řešení využijí spíše vetší společnosti, které ještě na virtualizovanou infrastrukturu nepřešli nebo rostoucí společnosti, které chtějí svou virtuální infrastrukturu rozšířit.

3.2.3 O2 Cloud

O2 je novým řešením mezi cloud systémy. „Nabízí technické zázemí a zařízení umístěné v hostingovém centru Nagano.“ [9]

U O2 Cloud je možné vytvářet také virtuální PC a servery. Toto cloudové řešení by mělo být vhodné pro malé a střední firmy, takže se nezaměřuje na velké korporace, ale spíše na menší podnikatele. Tímto se jim snaží zpřístupnit komfort, jakým cloud je. Na webu O2 jsem se moc nedověděl, ale po dalším hledání jsem našel, že celý jejich cloud, mimo jiné, poskytovaný jako služba, je založen na software od VMwaru. Na webu O2 jsou zmíněny pouze obecné informace o cloud systémech, zálohování cloud systémů, garance SLA a o tom, že všechny procesy jsou řízeny podle standardů ITIL atd. Po vyhledání na jejich stránkách jsem našel, že jsou partnerem VMware a získali nejvyšší certifikaci v oblasti cloud computing. Mezi jejich hlavní výhody, které bych shrnul v bodech, patří:

- „spolehlivost (hardware je umístěn v nejmodernějších datových centrech jako je Nagano a další, s úrovní bezpečnosti TIER 3+)
- jednoduchá správa (nastavení a ovládání probíhá prostřednictvím webového portálu O2 Cloud)

- rychlost (služby je možné aktivovat prakticky ihned)
- vysoká kapacita (v případě potřeby je možné okamžitě navýšit výpočetní či datovou kapacitu)
- podpora (nonstop odborná podpora pro všechny zákazníky)
- cena (cloud služby O2 zpřístupňují IT infrastrukturu firmám, které na ně zatím neměly finanční prostředky, a zlevňuje ji pro firmy, které zatím provozovaly vlastní řešení)“ [10]

Ve zkratce lze tedy říct, že O2 má „svůj“ cloud založený na softwarovém řešení od VMware, přesněji se jedná o produkt vCloud Director,

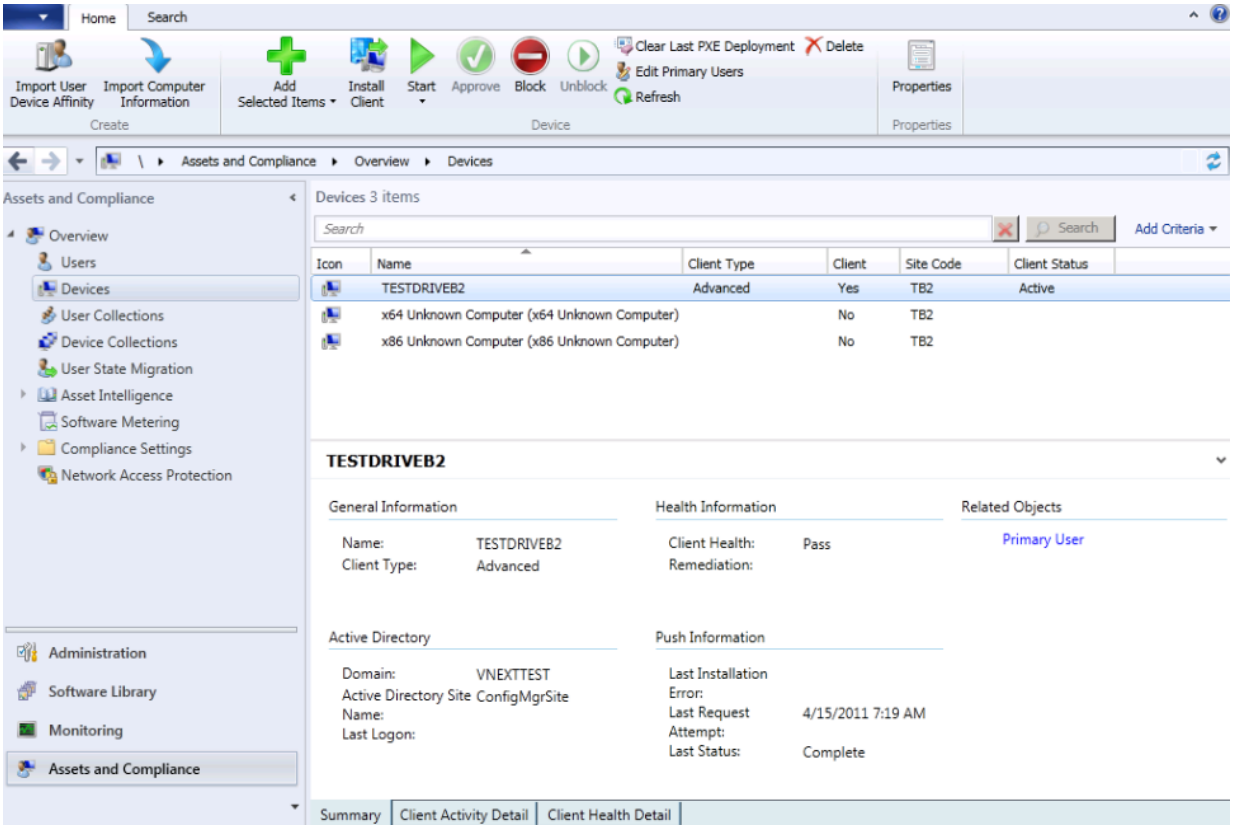
3.3 Varianty řešení od Microsoft

3.3.1 Private cloud – řešení Systém Center 2012

Cloud produkt je označen u Microsoftu pod názvem Microsoft Systém Center (dále jen SC) 2012. Skládá se z komponent – Orchestrator, Virtual Machine manager, App Controller, Operation Manager, Configuration Manager, Service Manager, Data Protection Manager. Orchestrator umožňuje automatizovat vytváření, monitorování a využití zdrojů ve virtuálním prostředí. Virtual Machine Manager poskytuje management pro virtuální počítače a zajištění služeb, které jsou nutné pro provoz private cloud. App controler poskytuje služby pro veřejný a private cloud. Tyto služby zajištují jednoduchou práci a konfiguraci virtuálních počítačů pro klienty cloud. Operation Manager poskytuje diagnostiku a monitoring infrastruktury k lepšímu využití hardwarového výkonu a kontroly funkčnosti datového centra. Configuration Manager slouží ke konfiguraci práv jednotlivých uživatelů a jejich přístupu jednotlivým virtuálním aplikacím. Service manager poskytuje postupy pro řešení problémů a také řeší mimořádné situace, které mohou nastat při provozu virtuální infrastruktury. Data Protection Manager poskytuje jednotnou ochranu dat pro servery Windows a klientské operační systémy. Tímto dodává efektivní ochranu jako například obnovení dat z disku, pásky atd. Na obrázku 3.5 je zobrazeno prostředí System Center 2012 [11].

Rozhraní pro prací s virtuálními PC je rozděleno do čtyř oddílů:

- **Administration -** správa a konfigurace systému
- **Software Library -** distribuce aplikací, aktualizací a operačních systémů
- **Monitoring -** monitorování výstrah systému, statusových událostí, SRS reportů
- **Assets and Compliance -** správa aktiv (uživatelů, zařízení, kolekcí …)



Obrázek 3.5 - System center 2012

V rámci poskytování IT služeb uživatelům je možné, na základě požadavků na zprovoznění IT služby nebo dodání aplikace, poskytnout tuto službu na všechny prostředky, které jsou ve správě IT oddělení této služby. Tato služba se v SC nazývá User-centric Managment.

„Příklad užití: Pokud má uživatel např. stolní počítač, mobilní počítač a chytrý telefon a požádá o aplikaci běžící na všech zmíněných platformách, je mu tato aplikace doručena na všechna zařízení současně, nebo na základě nastavení priorit pouze na preferovaná zařízení.“ [12]

Aplikační model SC Configuration Manager 2012 umožňuje, že aplikace může mít více možností nasazení – balíček MSI nebo App-V a aplikace pro mobilní zařízení (Windows Mobile Cabinet nebo Nokia SIS/JAR).

Aplikace samotné je možné také publikovat do webového portálu SC Configuration Manager 2012 nebo pomocí integrace do webového portálu SC Service Manager 2012. Uživatel si bude moci aplikaci nainstalovat zcela sám nebo mu bude na základě dalších pravidel po schválení nainstalována. Pro přístup k webovému rozhraní v SC je nutné mít nainstalovaný Application Catalog web service point a Application Catalog website point.

Private cloud si mohou klienti Microsoftu zprovoznit na svých stávajících datacentrech, které ovšem musí splňovat minimální požadavky pro provoz, které jsou stanoveny Microsoftem.

3.3.2 Public Cloud – Windows Azure

Windows Azure je cloud platforma, která umožňuje vytvářet, nasazovat a spravovat aplikace přes webové rozhraní v rámci globální sítě datacenter společnosti Microsoft a jejich partnerů. V prostředí Windows Azure lze psát vlastní aplikace a samozřejmostí je vytváření virtuálních PC s širokou škálou operačních systémů. Windows Azure, jako operační systém, využívá pro provoz těchto pět služeb:

- Live Services (zahrnuje většinu cloud aplikací)
- SQL Azure (uchování dat, úložiště, apod.)
- AppFabric (zahrnuje služby týkající se přímé funkce systému)
- SharePoint Services (webový portál)
- Dynamics CRM Services (služba sloužící ke zlepšení komunikace/vztahů se zákazníky)

Microsoft nabízí také možnosti propojení private cloud s public cloud.

3.4 Srovnání řešení VMware a Microsoft Cloud

V této kapitole bych chtěl srovnat dvě rozdílné společnosti dodávající svůj software pro provoz cloud systémů. Před začátkem bych chtěl říci, že jsem procházel různé zdroje a snažil se porovnat různé principy řešení jednotlivých platforem. Z teoretických poznatků usuzuji, že VMware sází spíše na techno-logičtější podporu tak, aby platforma uměla co nejvíce. Zatímco Microsoft jde principiálněji, zabývá se optimalizací procesů cloud systémů atd. Microsoft má řešení virtualizace založeno na systému Hyper-V.

Pro srovnání základních vlastností cloud slouží obrázek 3.6, který znázorňuje, jak řeší klíčové vlastností virtualizace jednotlivé platformy. Každá platforma pojmenovává své řešení svým názvem. V konečném srovnání řeší obě platformy tu samou věc, viz. obrázek 3.6.

Pro lepší porozumění jednotlivým funkcím přikládám jejich popis:

Vysoká dostupnost (HA) – charakterizuje zajištění prostředků (hardware) pro provoz cloud systémů, při výpadku části hardware

Neplánovaný výpadek – zajištění prostředků pro provoz cloud infrastruktury proti výpadkům a chybám

Resource planning – plánovaní zdrojů na virtualizační platformě

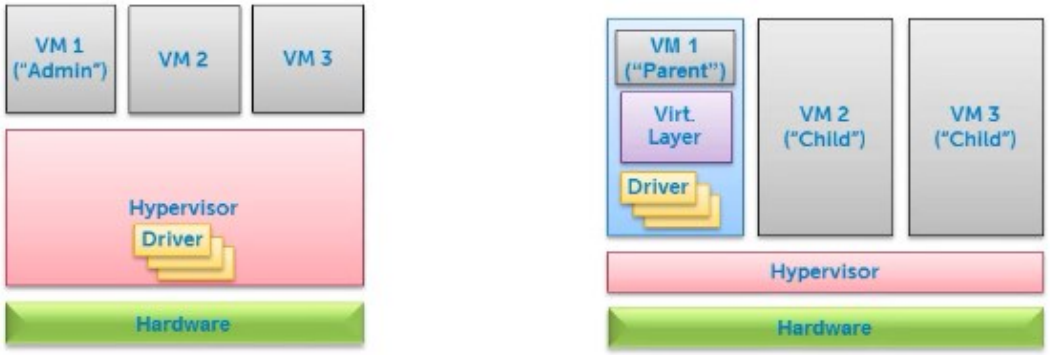
VM Migration – migrace v rámci vysoké dostupnosti (HA) mezi jednotlivými hostiteli

Memory plannign - plánování zdrojů paměti

Popis	VMware	Hyper-V
Vysoká dostupnost	High Availability (HA)	Windows Cluster
Neplánovaný výpadek	Fault Tolerance	
Resource planning	Dynamic Resource Scheduling (DRS)	Performance Resource Optimization (PRO)
VM Migration	VMotion	Live Migration Quick Migration
Memory planning	Memory Overcommit	Dynamic Memory

Obrázek 3.6 - „Srovnání klíčových funkcí platforem VMware a Microsoft“ [30]

Rozdíl mezi platformami VMware a Microsoft je v jejich hypervisorech. To ukazuje obrázek 3.7.



Obrázek 3.7 - „Hypervisory, vlevo VMware, vpravo MHyper-V(Microsoft)“ [30]

Vlevo je zobrazena architektura VMware a vpravo je zobrazena architektura Hyper-V. Velký rozdíl je v hypervisorech obou platforem a umístění ovladačů. U VMware jsou nahrány drivery přímo v hypervisoru, proto je nutné před výběrem hardware zjistit, zda jsou na seznamu kompatibilních serverů a jejich komponent. Hypervisor zabírá 32MB a je psaný v jazyce C.

U Hyper-V je zavedena takzvaná „parent partition“, na které běží virtuální PC s operačním systémem Windows Server a jsou v ní uloženy i drivery. Tato partition slouží také k managementu celého Hyper-V. Díky tomu je možné spustit virtualizaci na jakémkoli hardware certifikovaném Windows serverem. Současně je zajištěna širší podpora hardwarových komponent oproti VMware. Hypervisor u Hyper-V zabírá 707 KB. Srovnání vlastností ukazuje tabulka 3.1.

ESXi	Hyper-V
Větší Hypervisor / Menší platforma	Menší hypervizor / Obsáhlejší podpora
Podporuje Solaris	Bez podpory Solaris
Větší škálovatelnost pro velké implementace: více podporovaných aplikací – déle na trhu	Mladší platforma, méně podporovaných aplikací – nyní například i certifikovaný SAP a Oracle
32 MB – Hypervisor	Do 1MB hypervisor

Tabulka 3.1 - Vlastnosti hypervisorů

Při výkonnostních testech se testovaly obě platformy na serverech DELL PE M600 BLADE s hardware složením:

2x Quad Intel XEON 5450

16GB RAM

2x SAS 146 GB RAID

Tento server je na seznamech kompatibilních zařízení obou platforem. Testy probíhaly nástroji PassMark V7. PassMark slouží pro referenční testování systému a testovaní hardware.

Výsledek těchto testů potvrdil, že obě platformy se hodí do prostředí, která jsou na virtualizaci závislá.

Virtualizace může obecně přinášet mnoho výhod, avšak řešení virtualizace od společnosti VMware jsou postavena na spolehlivém základě ověřeném v provozních prostředích. Tato řešení jsou založena na nejmodernější virtualizační platformě VMware vSphere. Já osobně jsem měl se softwarem od VMware velice dobré zkušenosti. Ve své práci hodně testuji software a hojně k tomu využívám virtuálních PC založených na VMware. Z tohoto důvodu jsem si také vybral ke své diplomové práci řešení od VMware.

4 VMware - řešení virtualizace

Už delší dobu jsem využíval virtuální řešení od VMware a jak po stránce konfigurační, tak po stránce technické, splnil vždy mé pracovní nároky. Proto budu v této kapitole popisovat jeho základní vlastnosti a funkcionalitu. Pro pochopení celé komplexnosti softwaru od VMware je nutno začít od začátku. Část, na které je celá virtualizace založena, je takzvaný ESXi software, který se instaluje na jednotlivé PC a jejich výpočetní výkon je poté využíván pro virtuální prostředí. Více ESXi serverů mezi sebou spravuje VMware vCenter server, což je vlastně software pro management ESXi serverů, který tak vytváří centralizované prostředí pro konfiguraci a automatické řízení jednotlivých ESXi serverů. ESXi serverů bývá vždy více, aby při výpadku mohl přejít provoz virtuálních PC na jiný ESXi server a zabránilo se tak výpadku v reálné produkci. Nutno podotknout, že při mých testech jsem užíval prostředí vSphere ve verzi 5.1. Verze systému ESXi serverů byla také 5.1 [13].

4.1 Rozdíl mezi systémy ESX a ESXi

Před verzi systému ESXi, byl systém ESX, který se od stávajícího systému lišil architekturou a způsobem správy. Oba systémy poskytují špičkový výkon a škálovatelnost. Systém VMware ESX využívá k provádění některých administračních funkcí, kam patří spouštění skriptů a instalace agentů pro sledování hardwaru, zálohování či správu systému od jiných výrobců, operační systém Linux, zde nazývaný servisní konzole. V systému VMware ESXi byla servisní konzole odstraněna, čímž se výrazně omezila jeho velikost. Odstraněním servisní konzole systém VMware ESXi dovršuje současný trend migrace správy z místního rozhraní příkazového řádku na vzdálené nástroje pro správu.

Systémy VMware ESX a VMware ESXi se instalují přímo na hardware serveru, kde mezi hardware a operační systém virtuálních PC vkládají robustní virtualizační vrstvu. VMware ESX a ESXi dělí fyzický server na řadu bezpečných a přenositelných virtuálních strojů, jež mohou na jednom fyzickém serveru běžet současně. Každý virtuální stroj představuje kompletní systém s procesory, pamětí, připojením k síti, úložištěm a systémem BIOS. Operační systém a softwarové aplikace tak lze ve virtuálním stroji nainstalovat a provozovat bez jakýchkoliv úprav. Dále jsou virtuální stroje od sebe zcela odděleny virtualizační vrstvou, díky níž se pád aplikace nebo chyba konfigurace v jednom virtuálním stroji neprojeví v ostatních strojích.

Sdílením prostředků fyzického serveru mezi virtuálními stroji se zvyšuje využití hardwaru a výrazně omezují investice. Provoz přímo nad hardwarem dává systémům VMware ESX a ESXi plnou kontrolu nad prostředky serveru, přidělenými jednotlivým virtuálním strojům a umožňuje výkon

virtuálních strojů blízký fyzickým strojům a škálovatelnost podnikové úrovně. Systémy VMware ESX a ESXi poskytují virtuálním strojům vestavěné funkce pro vysokou dostupnost (HA), správu prostředků a bezpečnost, s nimiž dokáží softwarovým aplikacím poskytovat vyšší úrovně služeb než statická fyzická prostředí.

4.2 vSphere client – managment software

Pro konfigurace a nastavení prostředí ESXi serveru slouží takzvaný vSphere client. Uživatelské rozhraní nástroje VMware vSphere Client umožňuje společnou správu systémů VMware ESX a ESXi, virtuálních strojů a (volitelně) systémů VMware vCenter Server. Nástroj vSphere Client lze bezplatně stáhnout. Nabízí připojení k hostiteli VMware ESX či ESXi a správu jednoho hostitele, nebo připojení k systému vCenter™ Server a správu více hostitelů. Do vSphere lze instalovat mnoho pluginů a rozšíření, kterými jsou například vCloud Director, vSphere Storage Appliance (zkráceně VSA) atd. Plugin vCloud je nadstavba pro řízení cloud systémů, která rozšiřuje vCenter o webové rozhraní. Práce v prostředí vCloud je přizpůsobena pro definování klientských účtů firmám pro spravování vlastních (pronajmutých) virtuálních prostředků.

4.3 Virtuální přepínače

VMware je komplexní nástroj pro zvirtualizování nejen samostatných PC, na kterých lze provozovat různé systémy jako je například Linux – Ubuntu, Red Hat, Windows – Server 2008, Win 7, Win 8 a mnoho dalších. Jednotlivé virtuální počítače a servery lze spojovat do libovolných sítí, které si lze vytvořit. Spojkou mezi virtuálními počítači jsou zde virtuální přepínače. Mezi nejzákladnější, které zde popíši, patří vSwitch [14]. Dalším stupněm je Distributed Switch a posledním přepínačem je NEXUS 1000v od společnosti Cisco. První dva přepínače jsou tedy standardně obsaženy ve vSphere, třetí je nutné po registraci stáhnout ze stránek společnosti Cisco a následně nainstalovat. Cisco NEXUS přepínač lze vyzkoušet na 60 dní zdarma.

4.3.1 Vlastnosti virtuálního přepínače

S popisem vlastností jsem začal u základního virtuálního přepínače - vSwitch. Pro Distributed Switch platí tyto vlastnosti také, ale lze je trochu pokročileji nastavit. Mezi nejzákladnější vlastnosti vSwitch patří:

1. Počet virtuálních portů - parametr definující počet portů pro připojení virtuálních PC do vSwitch [14]

2. Hodnota MTU – maximální velikost rámce – tato hodnota je standardně 1500

3. Promiscuous mode – mód, který dovoluje odchytávat pakety z místní sítě

4. MAC address changes – kontrola změny MAC adresy virtuálního PC, pokud je odlišná od původní uložené, zahazují se příchozí pakety

5. Forged transmits – kontrola změny zdrojové MAC adresy virtuálního PC, pokud je odlišná od původní uložené, zahazují se odchozí pakety

6. Traffic shaping - zpožďování paketů při překročení definované rychlosti. Zde je možné definovat průměrnou přenosnou rychlost, dále také hodnoty špičky (Peak Information Rate - PIR) a také množství dat (Burst size), které je možné maximálně přenést, než se aplikuje traffic shaping. Konfigurace traffic shaping je zobrazena na obrázku 4.1.

7. NIC Teaming – můžeme dosáhnout navýšení propustnosti, kdy se komunikace podle určitých parametrů rozdělí a proudí přes různé fyzické síťové adaptéry. Dále získáme odolnost proti výpadku, kdy se komunikace přepne na záložní linku (nebo prostě přestane používat tu nefunkční). Obě tyto výhody jsou obzvlášť vhodné pro virtualizaci, protože jsme konsolidovali více serverů na jeden hardware. Navíc asi každý dnešní server má minimálně dvě síťové karty, a pokud ty další nepoužíváme k ničemu jinému (jako je například připojení k iSCSI), tak nás použití NIC Teamingu téměř nic nestojí (samozřejmě musíme mít zdroje jako port na přepínači apod.).

Ohledně NIC Teaming nastavujeme následující parametry:

Load Balancing - metoda, podle které dochází k vyvažování provozu na jednotlivé fyzické NIC (tedy přiřazení virtuálního Ethernet adaptéru uvnitř virtuálního PC přes vSwitch na fyzický Ethernet adaptér), možnosti jsou:

- Route based on the originated virtual port ID - NIC pro odchozí provoz se vybere podle ID portu na vSwitch, kam je zapojen virtuální PC, nejjednodušší a implicitní metoda. Provoz z virtuálního PC se posílá stále na jednu fyzickou NIC (pokud nedojde k výpadku) a odpovědi se očekávají z té samé NIC
- Route based on source MAC hash - podle posledního bytu MAC adresy, použité NIC u virtuálního PC (jeden virtuální PC může mít více NIC), se provoz z virtuálního PC posílá stále na jednu fyzickou NIC (pokud nedojde k výpadku) a odpovědi se očekávají z té samé NIC
- Route based on IP hash - podle spojení na IP úrovni, jednoduchý hash se počítá ze zdrojové i cílové IP adresy, virtuální PC může komunikovat přes více NIC, fyzický přepínač pak vidí stejnou MAC adresu na více portech, proto se doporučuje mít zapnut

statický EtherChannel[1], IP hash metoda by měla být nastavena na celý vSwitch a zděděna na všechny Port Group

- Use explicit failover order - zajišťuje pouze failover (odolnost proti výpadkům), NIC používá v daném pořadí a na další NIC předává provoz pouze při výpadku

Network Failover Detection - jakým způsobem detekuje přerušení linky

- Link Status Only – bere v úvahu pouze stav linky, jedná se o jednoduchou doporučovanou metodu
- Beacon Probing - odesílá do sítě broadcast[2] v každé VLAN a poslouchá, podle toho poté určuje funkční cesty

Notify Switch – odešle MULTICAST rámec se zdrojovou adresou z právě používaného portu, aby si přepínače aktualizovaly CAM[3] (Content Addressable Memory) tabulku, v případě kdy dojde k failover

Failback - pokud se sítový adaptér obnoví po chybě, tak se vrátí jeho aktivní funkce

Stejně, jako u NIC Teamingu ve Windows, máme dvě hlavní možnosti, jak Teaming nastavit. Od toho se také odvíjí, jaké prostředky budeme potřebovat:

- konfiguraci provedeme pouze na ESXi serveru - můžeme se připojit k libovolným typům přepínačů (to znamená i k jednoduchým bez managementu) a můžeme se zároveň připojit k různým přepínačům, vyvažování je pouze jednosměrné
- konfigurujeme-li ESXi server i přepínače - máme oboustranný Teaming, ale potřebujeme přepínač, který Teaming konfiguračně podporuje např. Cisco Catalyst, navíc pak musíme vést všechna spojení (na kterých se konfiguruje Teaming) do stejného přepínače

Ohledně detailů fungování NIC Teaming – při komunikaci s přepínačem dochází k přesunu MAC adresy na jednotlivých síťových adaptérech. Například u Management Network – k tomuto rozhraní přiřadí ESXi server MAC adresu prvního fyzického síťového adaptéru. Komunikace pak probíhá přes jeden síťový adaptér, pokud dojde k výpadku na této lince, tak se MAC adresa přesune na druhý fyzický síťový adaptér a komunikace pokračuje. Přepínač má vždy údaj, na kterém portu je tato MAC adresa, takže odpovědi posílá správně.

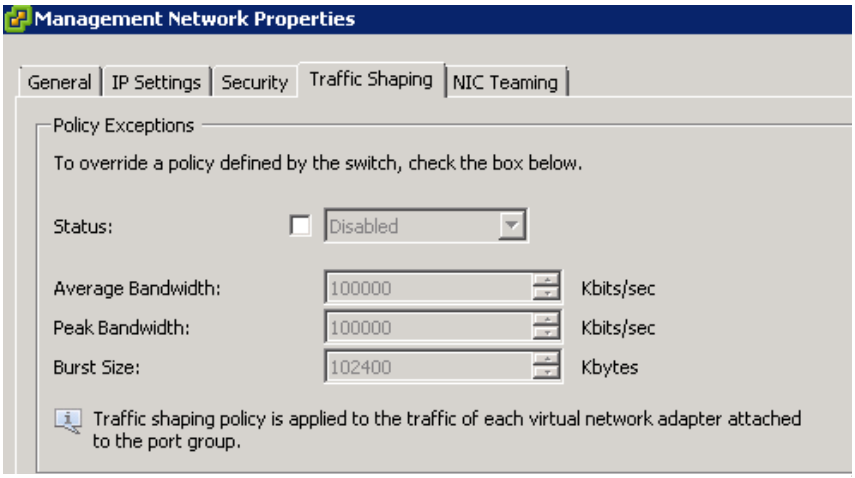
Když nastartujeme nějaké virtuální PC a začneme komunikovat po síti, tak se komunikace přiřadí k určitému fyzickému síťovému adaptéru (a zde se nastaví MAC adresa virtuálního PC). Toto přiřazení se může v průběhu různě měnit, pokud použijeme Load Balancing metodu Route based on IP hash. V případě výpadku se přesouvá na jiný funkční fyzický síťový adaptér. Pokud nepoužijeme

[1] EtherChannel je metoda, která zařizuje odesílání a přijímání dat přes více fyzických síťových adaptérů
[2] Broadcast je zpráva, kterou v počítačové síti přijmou všechna připojená síťová rozhraní
[3] CAM tabulka je to paměť, do které si přepínač zapisuje na kterém portu je která MAC adresa

EtherChannel [15], tak má přepínač MAC adresu přiřazenu vždy maximálně k jednomu portu a tam posílá komunikaci.

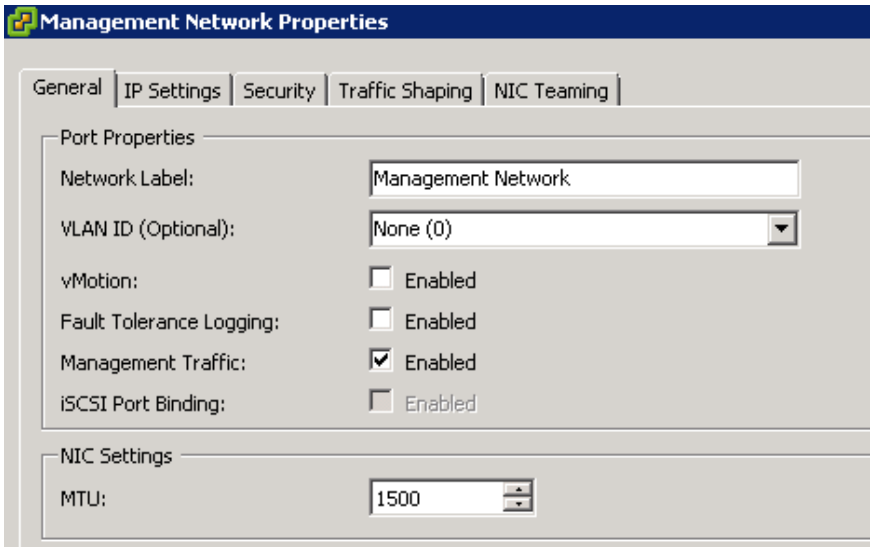
Na přepínači se objevují MAC adresy na jednotlivých portech, kde jsou připojeny fyzické síťové adaptéry. Pokud použijeme EtherChannel, tak nevidíme MAC na fyzických portech, ale pouze na virtuálním interface Port-channel. Tento interface má pod sebou fyzické porty a komunikovat může přes všechny (podle nastavené metody), MAC adresy má jakoby ke všem fyzickým portům [15].

V každém vSwitch můžeme nadefinovat různé podsítě. V nich lze také oddělovat komunikaci pomocí VLAN a také na každou aplikovat jiný traffic shapping. Nastavení traffic shaping je zobrazeno na obrázku 4.1. Kromě definování síti ve vSwitch, lze také nadefinovat takzvanou „VMkernel“ – což je síť pro systémovou komunikaci. Její konfigurace je zobrazena na obrázku 4.2. Používá se například u dvou a více ESXi serverů pro předávání provozních informací. Tyto informace jsou důležité například pro službu vMotion. Je vhodné oddělit jednotlivé sítě pro Management network, vMotion a Fault Tolerance Logging, jednak na úrovni fyzického adaptéru a také na úrovni port-group a VLAN ve vSphere. U „VMkernel“ lze definovat traffic shaping stejně jako u obyčejné sítě pro virtuální počítače. Port-group je skupina portů, pro kterou platí stejná síťová konfigurace.



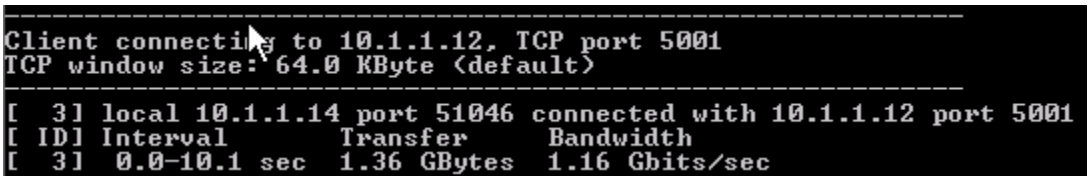
Obrázek 4.1 - Nastavení traffic shaping

Mé zkoumání bylo také zaměřeno na to, jak fungují a zda jsou jednotlivé servisní protokoly ve virtuální síti podporovány. Jedná se o protokoly STP, LACP, LLDP.



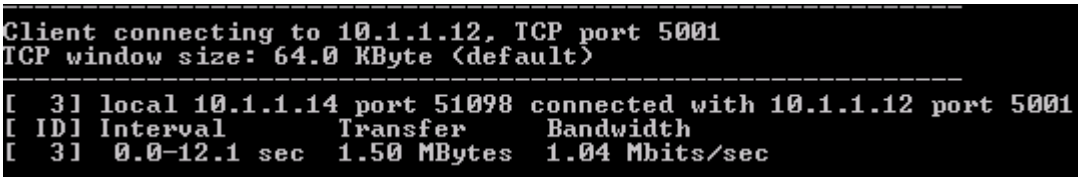
Obrázek 4.2 - Konfigurace „management network"

Pro ověření, zda tyto parametry dokáží nějak ovlivnit šířku pásma, jsem použil program Iperf, který důkladněji popíši v kapitole 5.2. Do vSwitch jsem připojil dva virtuální PC v rámci jednoho ESXi serveru. Nejdříve jsem otestoval šířku pásma bez omezení pomocí traffic shaping na vSwitch. Bez omezení jsem naměřil šířku pásma 1.16 Gbits/sec. Výsledky měření propustnosti zobrazuje program Iperf na obrázku 4.3.



Obrázek 4.3 - vSwitch bez nastavení omezení

Po nastavení traffic shaping – šířky pásma na 1000 Kbits/sec, hodnoty špičky také na 1000 Kbits/sec a „Burst size“ na 1000 Kbits/sec dostaneme korektní výsledek 1,04 Mbits/sec. Omezení propustnosti zobrazuje program Iperf na obrázku 4.4.

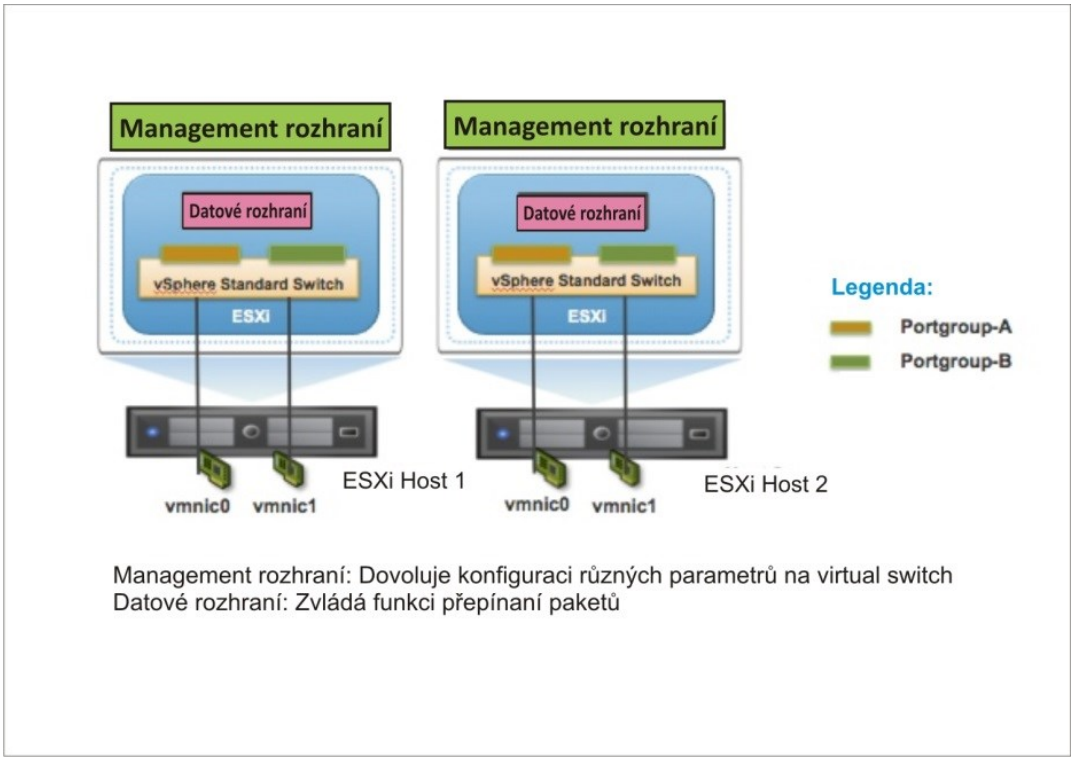


Obrázek 4.4 - vSwitch s nastaveným Traffic Shaping

Pro měření jsem použil protokol TCP s parametrem „windows size“ nastaveným na 64 KByte.

4.3.2 vSwitch

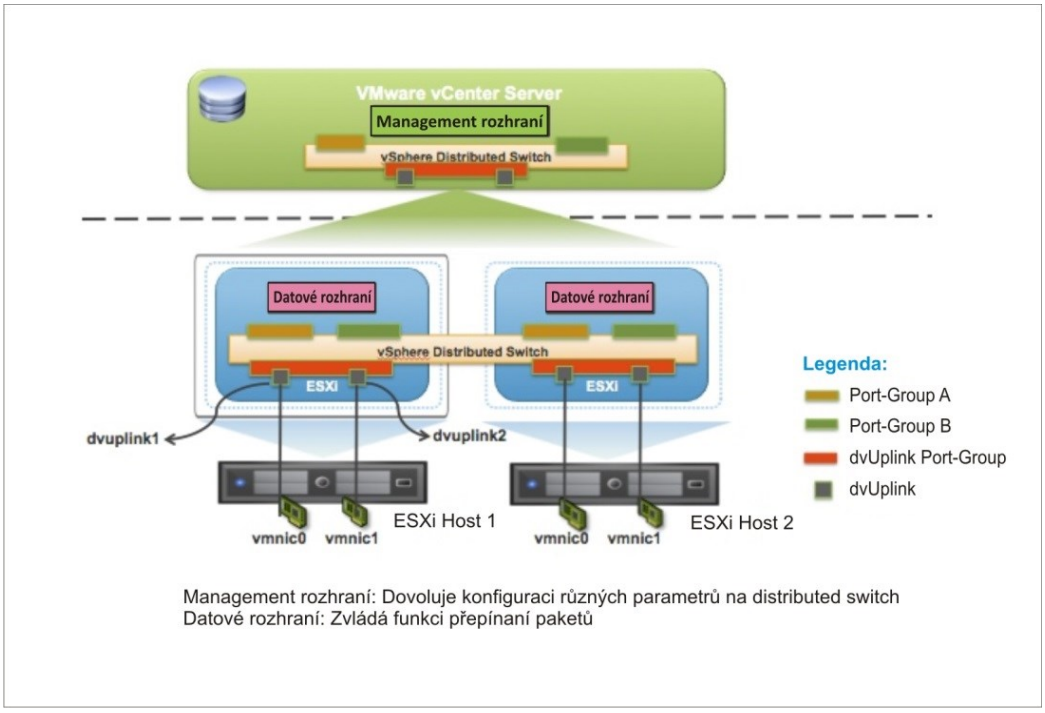
Nejzákladnějším virtuálním přepínačem je vSwitch. Jedná se o prostředí sítě, ve kterém si lze vytvořit svůj virtuální přepínač a jednotlivé virtuální PC do této sítě spojovat. Virtuální PC se připojují do sítě pomocí virtuálních adaptérů, jimiž jsou vybaveny virtuální PC. Lze tak vytvořit úplně izolované sítě, což je vhodné pro testovací prostředí. vSwitch lze vytvořit na fyzické síťové kartě, tudíž je pak celá virtuální síť připojená do reálné LAN. Konfigurace je opravdu pestrá, jednotlivé vSwitch lze přiřazovat do určitých VLAN a tvořit tak oddělené sítě jako v reálných systémech používajících VLAN. Lze tedy říci, že vSwitch má vlastnosti reálného přepínače na L2, neboť u něj lze nastavit mnoho dalších atributů, o kterých bych se chtěl zmínit v další kapitole. Každý fyzický síťový adaptér lze nastavit na požadovanou rychlost a duplexní spojení. Nutno podotknout, že fyzickým adaptérům nelze nastavit rychlost, na kterou nejsou přizpůsobeny. Tedy na síťový adaptér 10/100 nelze nastavit rychlost 1000, i když by ESXi servery měly mít takto rychlé síťové adaptéry. Virtuálním PC lze přiřadit virtuální síťový adaptér s jakoukoli rychlostí. K virtuálnímu PC lze přiřadit více než jeden virtuální adaptér. vSwitch lze vytvořit lokálně na jednotlivých ESXi serverech, ale nelze tímto přepínačem propojit virtuální PC jednotlivých ESXi serverů. Na obrázku 4.5 je vidět jak jsou interpretovány jednotlivé vSwitch na jednotlivých ESXi serverech [16].



Obrázek 4.5 - vSwitch

4.3.3 vSphere Distributed Switch (VDS)

Oproti vSwitch má VDS jednu velkou výhodu a to takovou, že lze spojit virtuální sítě jednotlivých ESXi serverů dohromady a vytvořit tak jednu společnou síť datacentra. Oproti vSwitch podporuje protokol LACP a dovoluje také rozšířené monitorování sítě pomocí nastavení port mirroring [24]. Port-mirroring je funkce, která umožňuje přeposílat provoz z určitého portu na jeden nebo více cílových portů. LACP protokol zde hraje velkou roli, protože při spojení sítí více ESXi serverů může poskytnout nutnou šířku pásma sítě, která je pro komunikaci dvou různých virtuálních PC
na jednotlivých ESXi serverech potřebná. Každá instance vCenter může podporovat až 128VDS a každý VDS může spravovat až 500 ESXi serverů. U VDS je situace rozložení datové a systémové komunikace jiná, oproti vSwitch. Datová komunikace probíhá samostatně v rámci jednotlivých ESXi serverů, ale systémová komunikace probíhá nad ESXi servery a řídí jí vCenter server. Obrázek 4.6 zobrazuje dvSwitch [16].



Obrázek 4.6 - Distributed Switch

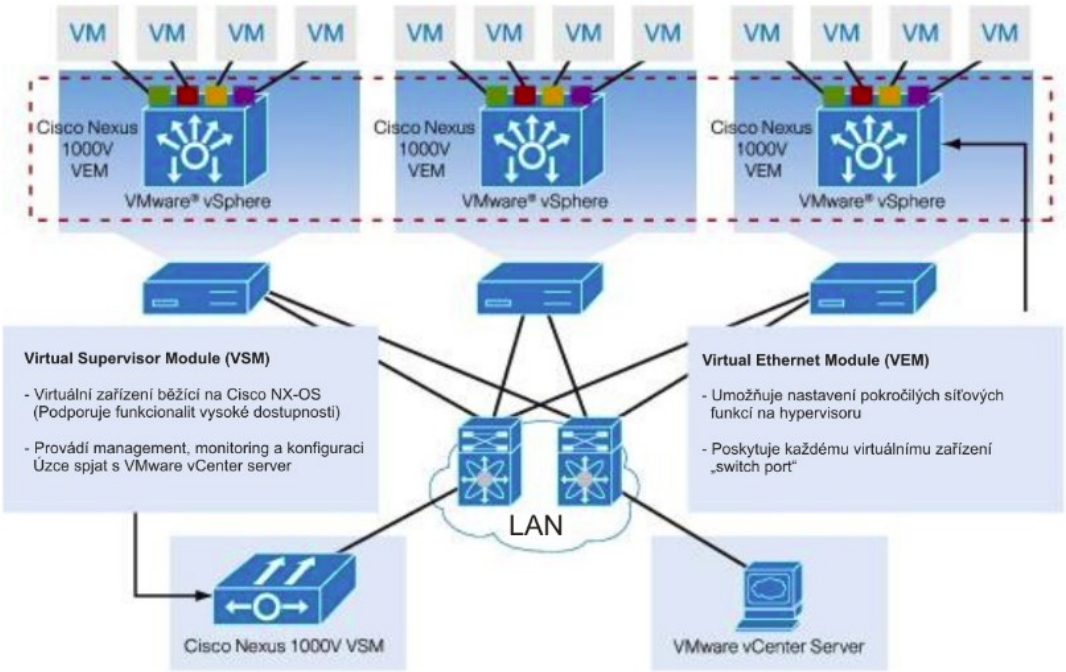
4.3.4 Cisco Nexus v1000

Jedná se softwarový přepínač integrovaný do kernelu ESXi serveru. Je to vlastně Distributed Switch na softwarové bázi. Toto softwarové řešení nahrazuje původní virtuální přepínač společnosti VMware uvnitř ESXi serveru. Nexus disponuje vlastnostmi v rámci virtuálního PC jako ostatní virtuální PC a stejně jako ostatní přepínače Cisco obsahuje systém Cisco IOS s telnet přístupem a CLI rozhraním. Také lze ve virtuální infrastruktuře využívat tradičních vlastností přepínačů s Cisco IOS

jako jsou spanning tree, Netflow, MAC address filtering a další. Konfigurace přepínače NEXUS je tedy odlišná od VDS a vSwitch, protože se konfiguruje přes příkazovou řádku jako všechny ostatní Cisco přepínače. K propojení všech ESXi hostitelských serverů je použit distribuovaný virtuální přepínač (Distributed Switch), který je řízen přepínačem Cisco Nexus 1000V. Poté Nexus řídí všechny fyzické síťové karty ESXi serverů a všechny porty virtuálního přepínače na všech ESXi serverech, jako kdyby to byl jeden síťový přepínač. Nexus je plně kompatibilní s VMware vCloud Director, což je technologie pro provoz webového cloud rozhraní. Nexus 1000v již podporuje Virtual Extensible Local Area Network (VXLAN). Se zavedením VXLAN na Nexus 1000V Series je možné síťě mezi virtuálními PC oddělovat nad rámec tradičních VLAN. Také jsou zde velké změny v propojení a škálovatelnosti NEXUS 1000v.

Software přepínače se skládá ze dvou částí. První částí softwarového přepínače je tzv. Virtual Ethernet Module (zkráceně VEM). Tento software poskytuje vlastní síťové služby pro každý virtuální PC uvnitř ESXi serveru. Druhou částí přepínače je tzv. Virtual Supervisor Module (VSM), software řídící všechny individuální moduly VEM. Konfigurace je prováděna pomocí Virtual Supervisor Module a automaticky propagována k modulům VEM. Místo konfigurace softwarových přepínačů uvnitř hypervisoru, pro každý hostitelský systém samostatně, lze definovat změny konfigurace pro všechny moduly VEM, které jsou spravovány pomocí Virtual Supervisor Module.

Oproti VD přepínači rozšiřuje NEXUS infrastrukturu o větší bezpečnost, škálovatelnost nastavení a také rozšířenější možnosti konfigurace. Mezi nejdůležitější rozšíření patří například private VLAN, ACLs a v neposlední řadě také možnost rozšíření load balancing. Na obrázku 4.7 je zobrazen přepínač NEXUS 1000v a znázornění jeho funkce uvnitř virtuální infrastruktury [17].



Obrázek 4.7 - „Cisco Nexus 1000v“ [27]

4.3.5 VXLAN

Společnosti Cisco a VMware navázaly strategické partnerství s cílem přinést společná řešení pro cloud infrastrukturu a virtualizaci desktopů. Hlavní novinkou vzešlou z této spolupráce je standard VXLAN, technologie virtuálních sítí. VXLAN – Virtual Extensible Local Area Network. Virtuální LAN přinášejí flexibilitu při alokaci dostupných zdrojů a mohou být vytvářeny „on-demand“. Tato technologie umožňuje vytváření milionů nezávislých sítí v rámci stávající infrastruktury a zjednodušuje tak implementaci a správu hybridních cloud systémů (spojujících private a veřejné cloud služby). Specifikace VXLAN je podporována v klíčových produktech, jakými jsou VMware vSphere 5, VMware vCloud® Director 1.5 či přepínač Cisco Nexus 1000V.

VXLAN je enkapsulační protokol, vytvářející překrývající síť na třetí vrstvě síťové infrastruktury. Dochází tedy k enkapsulaci (zapouzdření) L2 sítí do L3 paketů. Primárním cílem VXLAN je tedy rozšířit VLAN adresový prostor přidáním 24 bit segment ID (VNI) a zvýšit tak počet dostupných VLAN ID na 16 milionů. Segment VXLAN ID rozlišuje v každém svém rámci jednotlivé logické sítě, takže mohou existovat miliony izolovaných VLAN L2 sítí v L3 infrastrukturách. Stejně jako ve VLAN spolu mohou komunikovat pouze virtuální PC v rámci jedné logické sítě. Pomocí této technologie lze navýšit počet izolovaných síti. VXLAN lze vybudovat na stávající infrastruktuře s vCenter serverem.

4.4 Systémové Protokoly virtuálních přepínačů

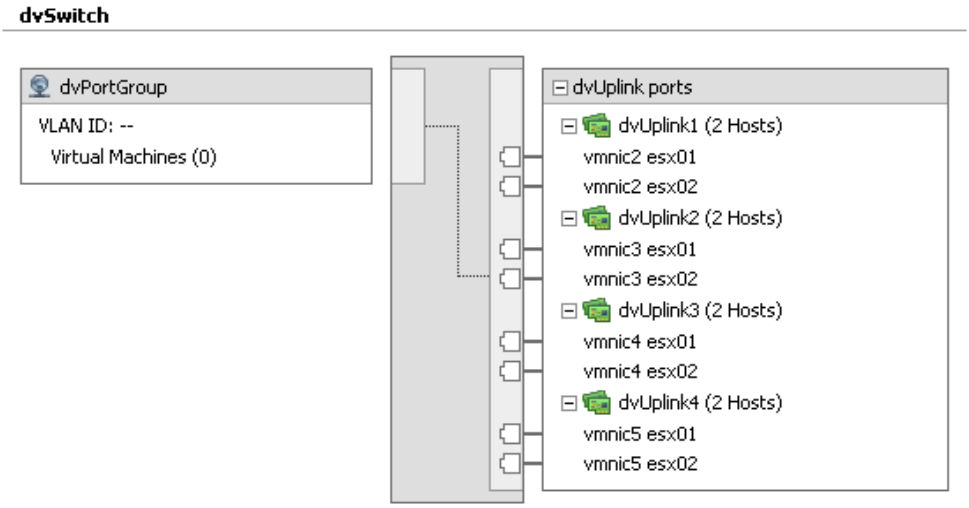
V této kapitole bych chtěl popsat jednotlivé protokoly, jejichž použití můžeme u virtuálních přepínačů najít.

4.4.1 STP – Spanning Tree Protocol

STP protokol slouží k tomu, abychom zabránili smyčkám v síti. Jeho algoritmus hledá nejkratší cestu mezi jednotlivými přepínači. Protokol STP není ve virtuálním přepínači přímo podporován, nicméně ve verzi vSphere 5.1 existuje takzvaný BPDU filtr. Tento filtr je u spojnice s lokální síti na ESXi hostiteli. Když BPDU filtr detekuje smyčku v síti, ESXi hostitel vyřadí fyzický síťový port, který je připojený k této síti. Poté bude komunikovat po jiném fyzickém síťovém portu (jiný port je připojen do jiného přepínače), dokud nedojde k nápravě chyby. Díky tomuto BPDU filtru je síť ochráněna například proti DOS útokům, které mohou vzniknout vysláním podvrhnutých BPDU paketů z virtuálního PC do lokální sítě. Na ESXi hostiteli jde nastavit, aby BPDU filtr kontroloval provoz, který jde i z virtuální infrastruktury, tedy lze filtrovat provoz oběma směry [18].

4.4.2 LACP – Link Aggregation Control Protocol

LACP protokol slouží k seskupení a ovládání více fyzických adaptérů, z nichž vytvoří jeden logický kanál. Toto seskupení slouží ke zvýšení šířky pásma. Důležitou podmínkou je, aby všechny síťové adaptéry byly stejného typu, se stejnou rychlostí a byly zařazeny do stejné VLAN nebo trunk[4] portu. Tento protokol je plně podporován na ESXi serverech, ale pouze u vSphere Distributed Switch. Obrázek 4.8 zobrazuje konfiguraci protokolu LACP [18].



Obrázek 4.8 - Popis fungovaní LACP

4.4.3 LLDP - Link Layer Discovery Protocol

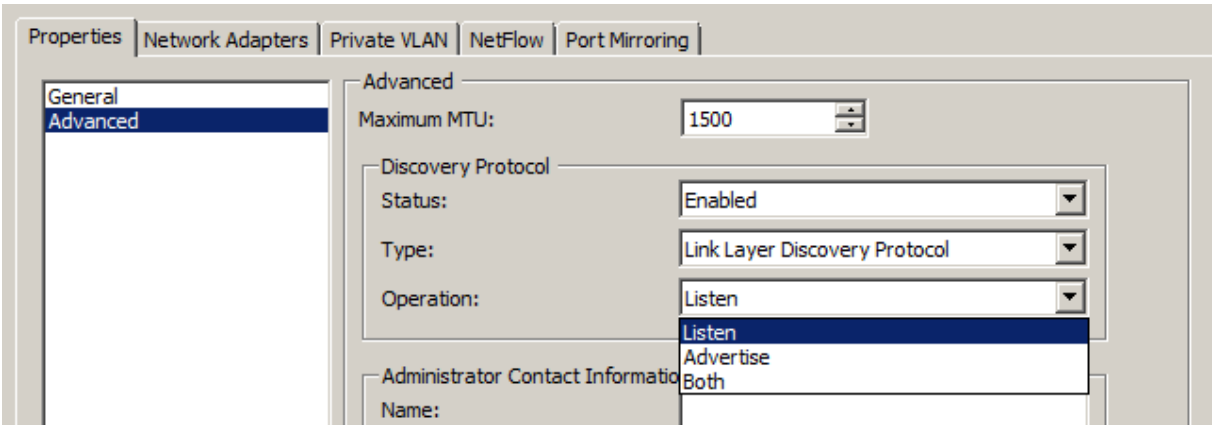
Link Layer Discovery Protocol je protokol spojové vrstvy. Je používán síťovými zařízeními k propagaci jejich identity, hlavních schopností a sousedů v IEEE 802 LAN, hlavně v Ethernetu. Informace distribuované tímto protokolem jsou uloženy v Management Information base (MIB) svých příjemců. K těmto informacím tak může přistupovat Network Management System (NMS) prostřednictvím management protokolu jako např. Simple Network Management Protocol (SNMP). S LLDP můžou vSphere správci určit, který fyzický port přepínače se připojuje k danému vSphere Distributed Switch (VDS). Protokol LLDP dovoluje na VDS zobrazit vlastnosti fyzického přepínače (např. ID, název systému a popis systému, a schopnost zařízení) a to vše z vSphere klienta. Prostředí pro nastavení protokolu LLDP [15] je zobrazeno na obrázku 4.9. Lze ho nastavit ve třech režimech:

1.Listen - ESXi server detekuje a zobrazuje informace o fyzickém přepínači, ke kterému je připojený, nepropaguje svou identitu fyzickému přepínači

[4] Trunk port je port, přes který se přenáší provoz všech VLAN, které jsou přepínači přístupné

2.Advertise - ESXi server propaguje svou identitu fyzickému přepínači, ale nedetekuje informace o fyzickém přepínači, ke kterému je připojený

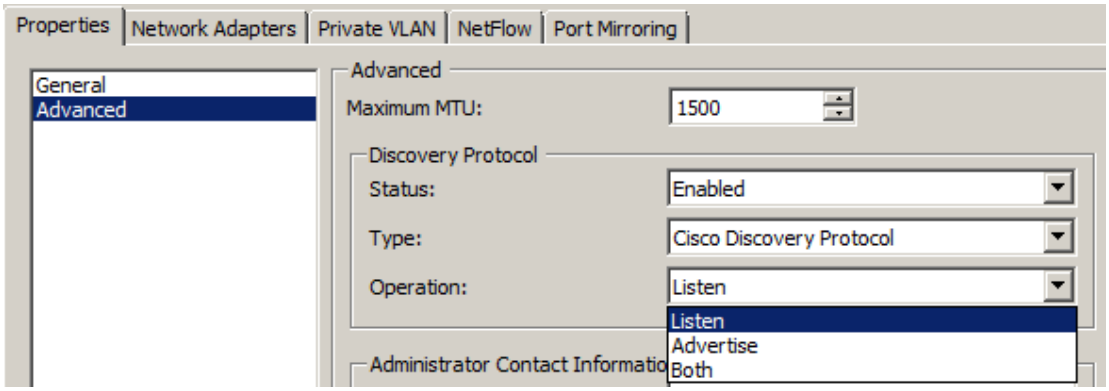
3.Both - ESXi server detekuje a zobrazuje informace o fyzickém přepínači, ke kterému je připojený a propaguje svou identitu fyzickému přepínači



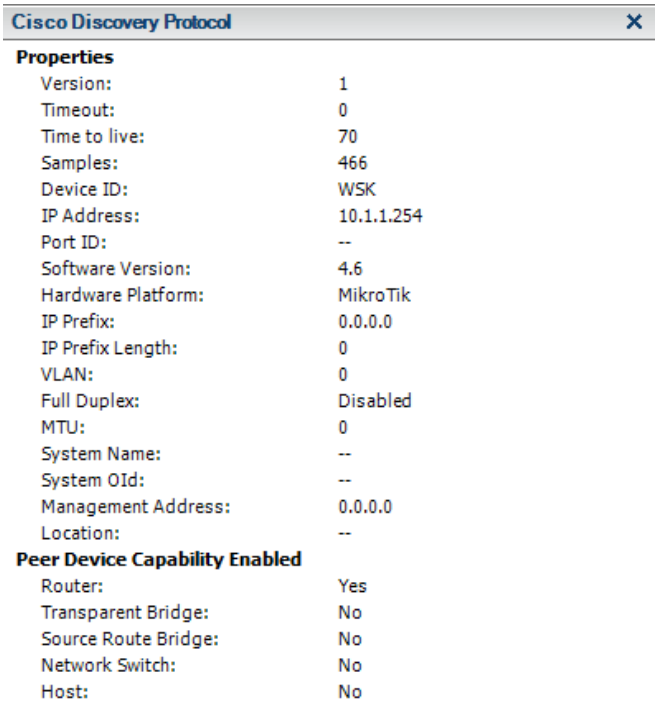
Obrázek 4.9 - Konfigurace LLDP distibuted switch

4.4.4 CDP – Cisco Discovery Protocol

Úkolem CDP je získávat informace ohledně přímo připojených Cisco zařízeních. Jedná se o proprietální protokol, který administrátorovi umožňuje získat souhrn informací jako IP adresa nebo protokol. CDP dovoluje ESXi administrátorům určit, který port z Cisco přepínače je připojen k vSwitch. Pokud je CDP zapnut, lze vyčíst u vSwitch ve vSphere klientovi informaci o přepínači jako je ID zařízení, verze software atd. CDP protokol lze nastavit ve třech režimech jako LLDP, tedy listen, advertise a both. Na obrázku 4.10 je vidět jak se konfiguruje CDP na ESXi serveru. Na obrázku 4.11 jsou zobrazeny informace, které CDP poskytuje.



Obrázek 4.10 - Konfigurace CDP u Distributed Switch



Obrázek 4.11 - CDP informace

4.5 Srovnání virtuálních přepínačů

Vlastnosti jednotlivých virtuálních přepínačů zobrazuje tabulka 4.1.

	VMware ESX 3.5 vSwitch	VMware vSphere vSwitch	VMware vSphere VDS	Cisco Nexus 1000V
Switching Features				
L2 Forwarding	✓	✓	✓	✓
VLAN Segmentation		✓	✓	✓
IEEE 802.1Q VLAN Trunking	✓	✓	✓	✓
Network VMotion (Port state follows VM)			✓	✓
VM Tx Rate Limiting	✓	✓	✓	✓
VM Rx Rate Limiting			✓	✓
NIC Teaming/Port Channels	✓	✓	✓	✓
LACP EtherChannel				✓
Multicast Support	✓	✓	✓	✓
Security Features				
Private VLAN			✓	✓
Access Control List				✓
Cisco Port Security				✓
VMware Port Security	✓	✓	✓	✓
VMSafe Compatibility		✓	✓	✓
Management Features				
Associate VMs to Network	✓	✓	✓	✓
Network Monitoring	✓	✓	✓	✓
Network Provisioning	✓	✓	✓	
-Standard IOS CLI **-Network Provisioning** **-XML API**				✓
Port Profile	✓	✓	✓	✓
Port Profile Inheritance				✓
SPAN				✓
VMware Port Mirroring (Promiscuous)	✓	✓	✓	
ERSPAN - Port Mirror Across L3 Boundaries				✓
Netflow v5	✓*	✓*	✓*	✓
Netflow v9				✓
SNMP v3 RW				✓
CDP v1/v2	✓	✓	✓	✓
Export to Syslog Server				✓
System Features				
Active/Standby Supervisor for Control Plane HIGH Availability				✓
SSH/Telnet				✓
VMware Remote CLI	✓	✓	✓	

Tabulka 4.1 - Vlastnosti virtuálních přepínačů

**Experimentální podpora*

Vysvětlení významů z tabulky 4.1:

ERSPAN - Port Mirror Across - funkce umožňuje sledovat provoz na jednom nebo více portech nebo ve více virtuálních sítích a přeposílat monitorovaný provoz na jeden nebo více cílových portů. ERSPAN může posílat provoz do síťového analyzátoru, sondy nebo jiného vzdáleného monitorování.

L3 Boundaries- hranice L3 k ohraničení L2.

Active/Standby Supervisor for Control Plane HIGH Availability – jedná se o službu kontrolující funkce, které zajištují vysokou dostupnost (HA) virtuálních zařízení ve virtuální infrastruktuře.

4.6 VMware vCenter server

VMware vCenter server poskytuje jednotnou správu všech hostitelů a virtuálních strojů v datacentru z jediného ovládacího panelu se souhrnným monitoringem výkonu clusterů[5], hostitelů a virtuálních strojů. VMware vCenter Server dává administrátorům podrobný náhled do stavu a nastavení clusterů, hostitelů, virtuálních strojů, úložiště, hostovaného operačního systému a dalších kritických prvků virtuální infrastruktury – vše z jednoho místa.

VMware vCenter Server usnadňuje správu virtualizovaných prostředí – jediný administrátor může spravovat 100 i více systémů.

vCenter server je systém, který umožnuje využít výkon všech ESXi serverů a přemísťovat jednotlivé virtuální PC na jiné ESXi servery. Dále lze využít funkcí jako je High Avaibility (HA), Distributed Resource Scheduler (DRS) a mnoho dalších. Přes vCenter lze vytvořit cluster z ESXi serverů a zamezit tak výpadku virtuálních PC. Například při výpadku jednoho z ESXi serverů lze pak jednoduše virtuální PC přesouvat z jednoho ESXi serveru na druhý. Zjednoduší se tak i údržba serverů [19].

4.7 VMware vCloud Director

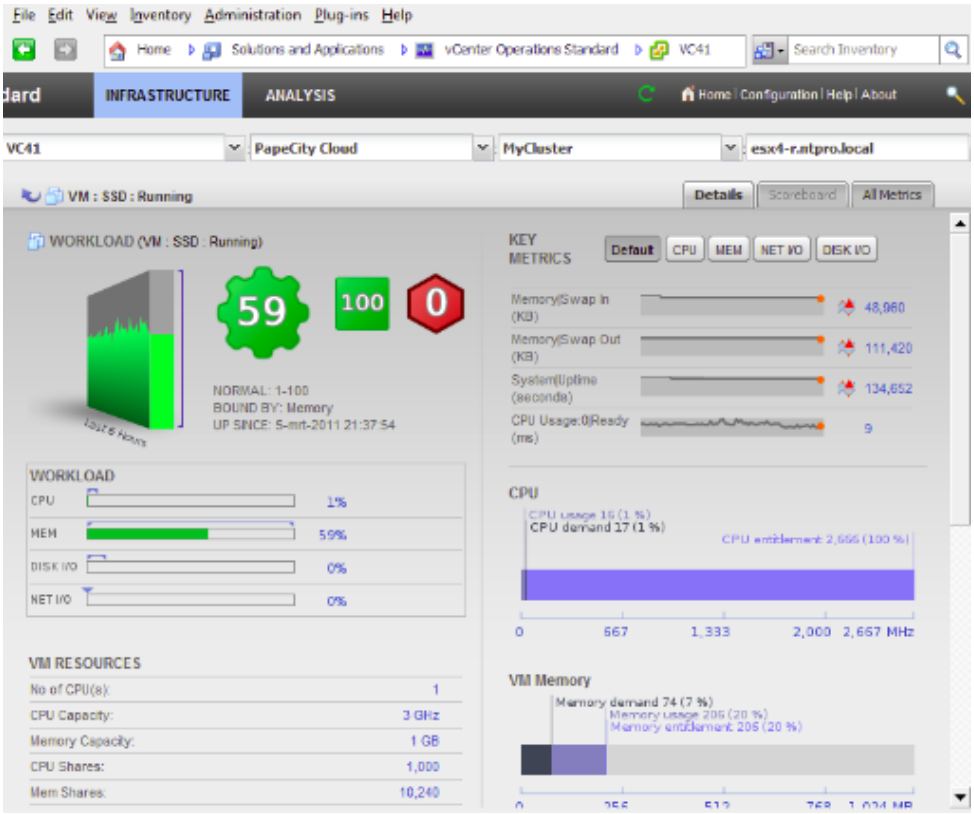
VMware vCloud Director sdružuje infrastrukturní zdroje napříč clustery do virtuálních datacenter dle definovaných pravidel. Možnost integrace s existujícím řešením vSphere a rozšiřující možnosti (např. VMware Distributed Resource Scheduler - DRS a VMware vNetwork Distributed

[5] Cluster je seskupení počítačů, které spolu úzce spolupracují, takže navenek mohou pracovat jako jeden počítač

Switch) VMware vCloud Director poskytují přizpůsobivé rozhraní pro výpočetní, úložná a síťová rozhraní napříč clustery.

4.8 VMware vCenter Operations

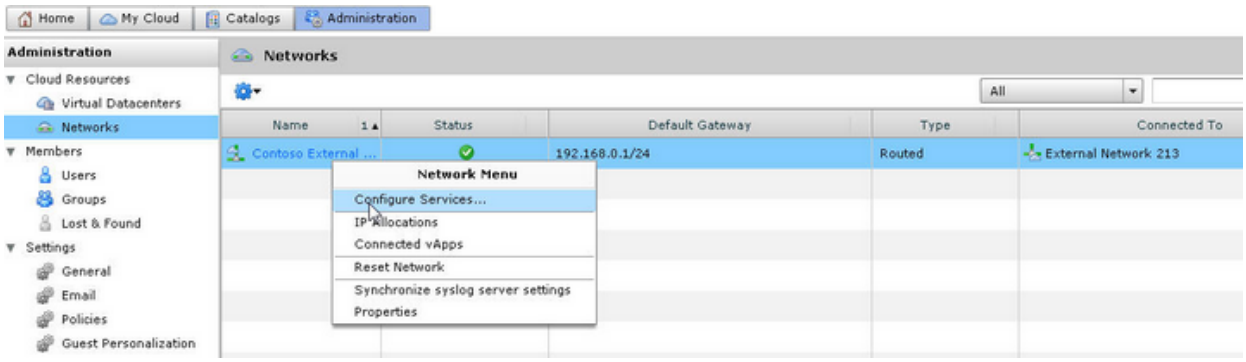
Tento produkt slouží pro dohled, monitorování a kapacitní plánování nad virtualizovanou infrastrukturou. vCenter Operations je plně integrovaný do vCenter serveru a tím umožňuje větší automatizaci procesů spojených s managementem virtuální infrastruktury. Také pomáhá administrátorům identifikovat vznikající problémy, případně identifikovat problémy s výkonem způsobeným konfiguračními změnami. VMware vCenter Operations jako takový je součástí balíku produktů, který se nazývá vCenter Operation Management Suite. Obsahuje funkcionalitu, která dokáže automaticky najít a zmapovat vztahy a závislosti mezi jednotlivými aplikacemi a částmi infrastruktury, které je podporují. To umožňuje administrátorům v rámci infrastruktury optimalizovat operace, jako je například nastavení bezpečnostní správy a obnovování následků po havárii na základě individuálních požadavků aplikací. Tento produkt je také vybaven automatickou analýzou zdroje problémů a také rozpozná problematické konfigurace napříč všemi vrstvami infrastruktury. Na obrázku 4.12 je zobrazeno prostředí vCenter Operations [20].



Obrázek 4.12 - „Ukázka monitoringu - vCenter Operations“ [25]

4.9 vCloud Networking and Security (vShield)

vCloud Networking and Security poskytuje služby jako je firewall, VPN koncentrátor, analýzu provozu, load balancing, VXLAN a další sítové služby pro provoz celého vCenter serveru. Jak již bylo zmíněno, tento komponent se instaluje naVMware vCenter server. vCloud Networking and Security běží na ESXi hostiteli stejně jako virtuální PC a slouží také k monitorování dalších komponent vCnter serveru. vCloud Networking and Security se konfiguruje přes webové rozhraní. Konfigurace virtuální sítě přes web je zobrazena na obrázku 4.13.



Obrázek 4.13 - „VMware vCloud Networking and Security – Konfigurace virtuální sítě“ [26]

Přes webové rozhraní vCloud Networking and Security lze také získat informace o struktuře datacentra a také informace o jednotlivých virtuálních PC.

Mezi klíčové vlastnosti této komponenty patří:

Firewall – lze zapnout pro celé virtuální datové centrum a lze také použít na jednotlivé virtuální síťové adaptéry, jednotlivých virtuálních PC. Ve správě Firewall je možno jednoduše nastavovat pravidla pro příchozí a odchozí provoz a automatizovat tak provoz vCenter serveru.

VPN – Datové centrum lze rozšířit o VPN. Tato VPN podporuje standardy jako IPsec a SSL VPN

Verze této komponenty vychází ve dvou edicích – Standard a Advanced. Edice Advanced obsahuje navíc oproti edici Standard funkcionalitu vysoké dostupnosti (High Availability) pro hraniční firewall, load balancing a bezpečnosti dat pro služby ve Windows.

5 Testování funkcí VMware

V této kapitole bych se chtěl zabývat provedenými testy sítě v prostředí VMware. Prováděl jsem například testy trunk portu ESXi serveru napojeného na Routerboard Mikrotik. Dále mě také zajímala udržitelnost nastavení omezení propustnosti na portu přepínače NEXUS 1000v a v neposlední řadě jsem se zabýval testy private cloud a VXLAN, STP, LACP.

Všechny testy jsem prováděl na dvou ESXi serverech s parametry, které zobrazuje tabulka 5.1.

	ESXi 1	**ESXi 2**
CPU	Intel(R) Core (TM) i7-3770 CPU @3.40GHz	Intel(R) Core (TM)2 Quad CPU Q9400@2.66GHz
Počet Socket procesoru	1	1
Počet jader procesoru	4	4
Logických CPU	4	4
Pamět (RAM)	16GB	8GB
Počet síťových karet	2	2
Uložiště	HDD 1TB, iSCSI diskj 2TB(RAID 1)	HDD 2TB, iSCSI disk 2TB(RAID 1)
Verze VMware ESXi	5.1.0 build-799733	5.1.0 build-799733

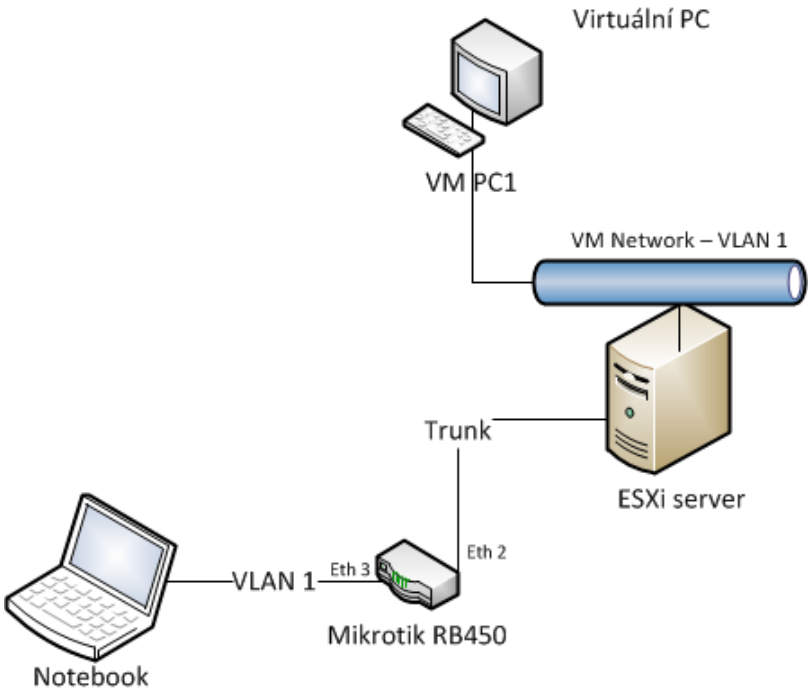
Tabulka 5.1- PC sestavy použité pro testování

Nejedná se o PC sestavy, které by byly do produkčního prostředí vhodné, nicméně musel jsem pracovat s hardware, který jsem měl k dispozici a který byl kompatibilní se software od VMware.

5.1 VLAN – propojení Mikrotiku a vSwitch - 802.1Q

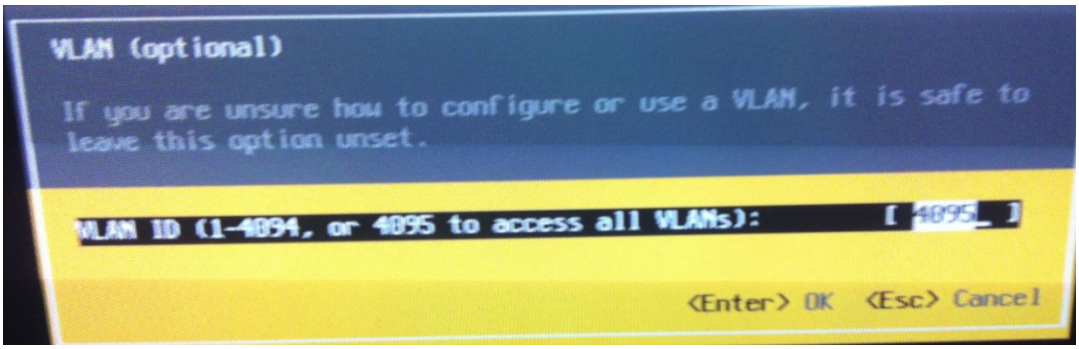
802.1Q [21] přináší mnohé - od prostého zvýšení počtu logických síťových rozhraní směšovačů, přes úspory na kabeláží a zflexibilnění koncepce sítí. Fungování 802.1Q je poměrně triviální – každý Ethernet rámec (pomineme-li native VLAN), který prochází přes trunk port, je označen značkou – to jsou čtyři byty ke každému rámci navíc. Dva byty obsahují tzv. ethertype, tedy hodnotu, podle níž zařízení pozná, že se jedná o rámec značkovaný podle normy 802.1Q. Zbylé dva obsahují jednak VLAN ID, tedy dvanáctibitové číslo samotné VLAN, a pak CoS (Class of Service), což je tříbitová hodnota, podle ní může, ale také nemusí (v závislosti na nastavení), být určitým

způsobem prioritizován provoz. S ohledem na 802.1Q uznáváme dva režimy provozu portů na síťových zařízeních – jednak tzv. přístupové (access porty), po nichž teče provoz již „neznačkovaný“ (typicky přepínač u odchozího rámce značku přidá a naopak, u příchozího rámce značku odstraní), a pak tzv. trunk, tedy porty, po nichž veškerý provoz (s výjimkou native VLAN) naopak „označkovaný“ teče. Schéma zapojení sítě pro test 802.1Q zobrazuje obrázek 5.1.



Obrázek 5.1 - Schéma zapojení sítě

Test proběhl následovně: na jedné straně byl ESXi server a na druhé straně byl Mikrotik Routerboard 450. ESXi server byl spojen s Mikrotikem UTP kabelem. Na ESXi serveru jsem nastavil na fyzickém rozhraní VLAN 4095, což je vlastně nastavení trunk portu. Nastavení přímo na ESXi serveru je zobrazeno na obrázku 5.2.

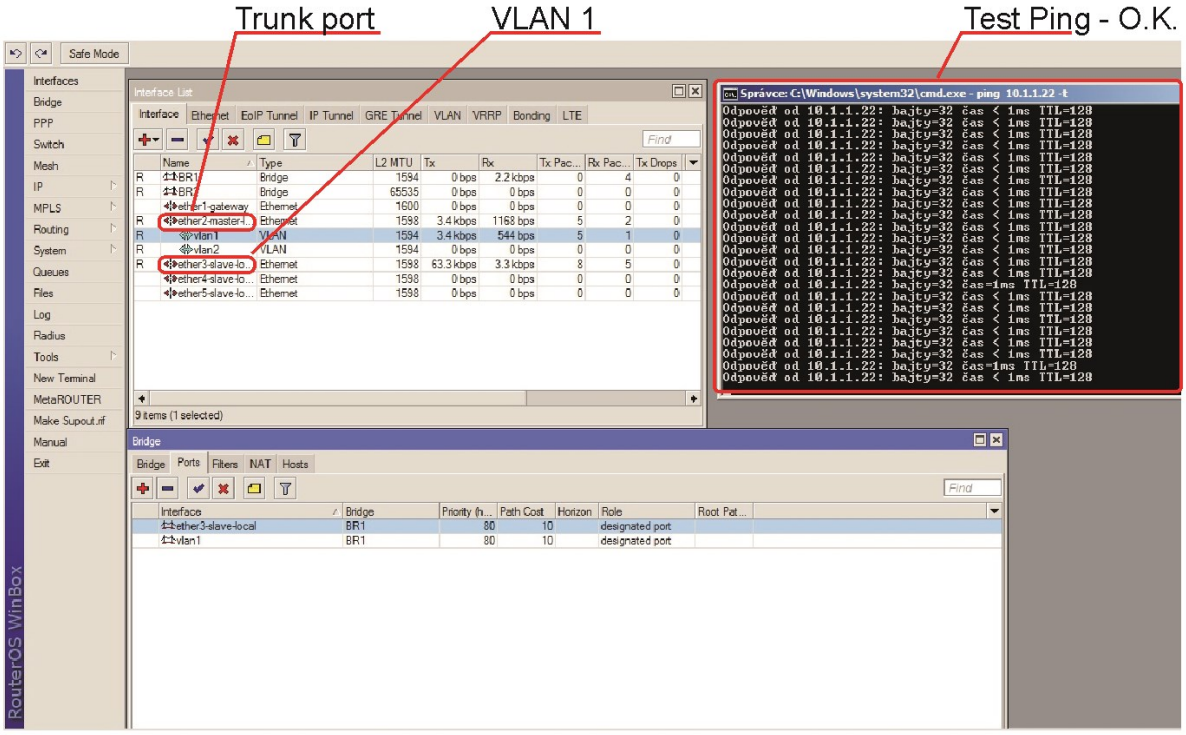


Obrázek 5.2 - Konfigurace ESXi hostitele – trunk port

6

6

Na Mikrotiku jsem nastavil trunk port na port ether2. Na ESXi serveru jsem nastavil pro virtuální PC VLAN 1 a na Mikrotiku jsem nastavil do bridge port ether 3 a VLAN s ID 1. Koncepce Mikortiku je zde taková, že je potřeba vytvořit bridge port pro NIC a VLAN. Virtuální PC má nastavenou IP adresu 10.1.1.208. Otestoval jsem spojení s virtuálním PC pomocí příkazu ping. –t. Toto lze vidět na obrázku 5.3.



Obrázek 5.3 - Konfigurace a test na Mikrotiku

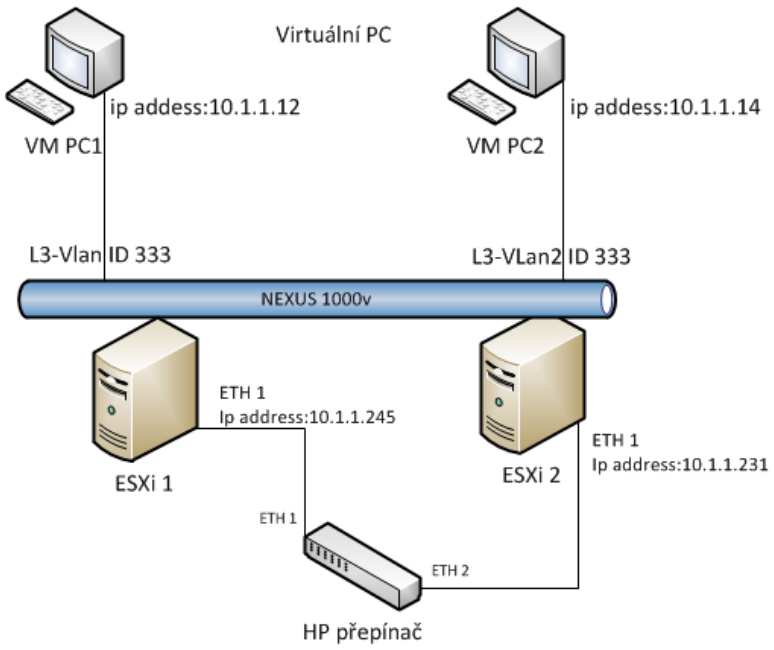
Pokud nastavíme v naší VLAN připojené k portu ether 3 na Mikrotiku – VLAN ID 2, dojde ke ztrátě komunikace s virtuálním PC. Příkaz ping neprojde, protože port ether 3 je nastaven VLAN ID 2 a ve virtuálním prostředí má VM network přidělenou VLAN ID 1. U VM network bychom museli změnit VLAD ID na 2 a poté by ping prošel.

Tento test ověřil, že lze kombinovat vSwitch z Vsphere a Mikrotik po propojení pomocí trunk portu. Mikrotik jsem zvolil z důvodu testu, zda bude kompatibilní komunikace se software od VMware.

5.2 Zachování parametrů QoS při migraci na NEXUS 1000v

Pro tento test jsem navrhnul topologii na obrázku 5.4. Jsou zde dva ESXi servery, které jsou připojené do HP přepínače. Nad oběma servery, ve virtuální infrastruktuře, je spuštěn přepínač

NEXUS 1000v. Na přepínači NEXUS jsem vytvořil dva port-profie, které jsou ve vSphere intepretovány jako port-group. Jeden port-profile se jmenuje L3-Vlan a druhý se jmenuje L3-Vlan2. Port-profile definuje nastavení pro určitý počet portů přepínače NEXUS. Na port-profile se natavuje například VLAN ID a také je možné nastavit určité omezení pro porty port-profile. Na obou port-profile je nastavená VLAN ID 333, aby mezi sebou mohli virtuální PC komunikovat. Virtuální PC 1 je spuštěno na ESXi serveru 1 a virtuální PC 2 je spuštěno na ESXi serveru 2. PC 1 je umístění v port-group/port-profile L3-Vlan a PC 2 je umístěno v port-group/port-profile L3-Vlan2.



Obrázek 5.4 - Schéma topologie s virtuálním přepínačem NEXUS 1000v

Na začátku bych chtěl popsat, jak přepínač NEXUS 1000V do vCenter server vůbec nainstalovat. Dá se nainstalovat dvěma způsoby. Nejdříve jsem zkoušel nejjednoduší způsob pomocí implementace souboru OVF (Open Virtualization Format) přes vSphere klienta. OVF soubor je vlastně balíček pro distribuci virtuálních PC. Přepínač NEXUS jsem instaloval ve verzi 4.2.1.SV2.1.1a. Po instalaci NEXUS se v vCenter server objeví přepínač NEXUS 1000v. Tento typ instalace je jednoduchý, nicméně po instalaci je nutné NEXUS 1000v nakonfigurovat přes Cisco CLI.

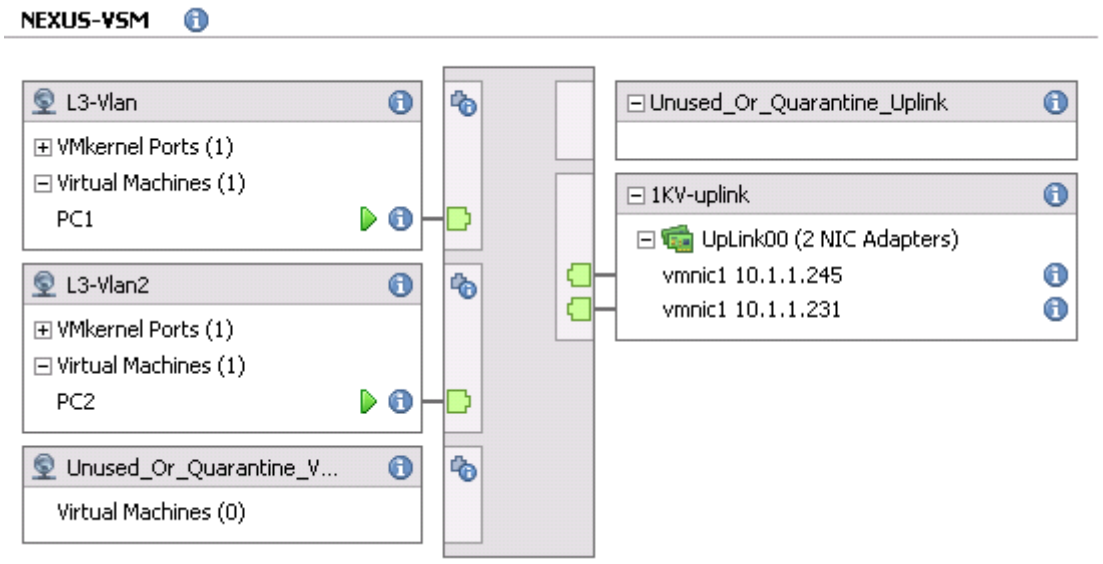
Přepínač Nexus 1000V lze instalovat do vCenter server také pomocí připraveného Java rozhraní. Toto rozhraní nainstaluje do vCenter vždy dva přepínače NEXUS – jeden hlavní a druhý záložní. Z důvodu testování pravidel QoS jsem zvolil, aby NEXUS komunikoval s vCenter server po L3.

Přepínač bylo nutné ještě dokonfigurovat ve vCenter serveru manuálně, v podobě vytvoření port-profile – ve vSphere se jedná se o port-group, jak bylo zmíněno na začátku. Tento port-profile je

implicitně definován pro 32 portů na přepínači NEXUS. Počet portů lze zadat i manuálně. Port-profile se vytváří přes Cisco CLI.

Vytvořil jsem si tedy topologii, která vypadá ve vSphere tak jako na obrázku 5.5. Na levé straně jsou zobrazeny port-profile rozhraní pojmenované jako L3-Vlan a L3-Vlan2. Dvě port-group jsem si vytvořil záměrně, abych mohl ověřit zachování nastavení omezení při změně portů na přepínači NEXUS, případně při migraci na druhý ESXi server. Tyto port-profile jsou ve stejné VLAN. Také je zde port-profile Unused_Or_Quarantine_Veth na levé straně a na pravé straně je Unused_or_Quarantine_Uplink. Tyto port-profile jsou vytvořeny na přepínači NEXUS 1000v implicitně. V každém port-profile je jeden testovací virtuální PC určený pro testy propustnosti. Na pravé straně jsou uplink porty jednotlivých ESXi serverů. Oba ESXi servery a jejich síťové karty spojuje přepínač NEXUS. Virtuální PC 1 je spuštěno na ESXi serveru 1 a virtuální PC 2 je spuštěno na ESXi serveru 2.

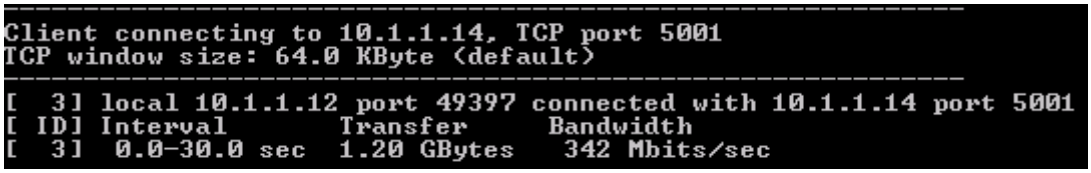
Pro testování propustnosti jsem využil program Iperf, který lze spustit buď jako server nebo jak klient. Iperf umí komunikovat jak po protokolu TCP, tak i po UDP. V mých testech jsem spustil Iperf pouze v režimu TCP, protože byl pro mé testy dostačující. Program Iperf lze spustit i s jinými parametry, jako je délka spojení, port na který se má připojit atd. Iperf server bude spuštěn na PC2 s IP adresou 10.1.1.14. Iperf klient bude na PC 1 s IP adresou 10.1.1.12. Iperf jsem spouštěl přes příkazovou řádku Microsoft Windows.



Obrázek 5.5 - Schéma sítě ve vSphere

Nejdříve jsem otestoval propustnost sítě, bez nastavení omezení na L3-Vlan port-profile, do kterého je připojen jeden virtuální PC1. Šířka pásma po změření je 342 Mbits/sec. Iperf testuje

propustnost po dobu 30 sekund a jako výsledek dá průměr šířky pásma za těch 30 sekund. Výsledek programu je zobrazen na obrázku 5.6.



Obrázek 5.6 - Iperf test propustnosti bez nastavení pravidel QOS

Poté jsem nastavil omezení QoS na přepínači NEXUS takto:

policy-map type qos class2 // Jedná se o QoS policy map se jménem class2

class class-default // Definice implicitní třídy

police cir[7] 380 kbps bc 200 ms conform transmit violate drop // Nastavení omezení na 380 kbps, pokud je tato hodnota překročena, dojde k zahazování provozu

Aplikování pravidla QoS na port-profile L3-Vlan je nastaveno takto:

port-profile type vethernet L3-Vlan // Definice port-profile na Cisco NEXUS 1000v

capability l3control // Nastavení portu, že může být ovládán L3

VMware port-group // Ve vSphere se jedná o port-group

switchport mode access // Jedná se o přístupový port

switchport access vlan 333 // Port má přístup do VLAN 333

service-policy input class2 // Aplikování QoS pravidla na příchozí provoz

service-policy output class2 // Aplikování QoS pravidla na odchozí provoz

no shutdown // Port nemá být vypnutý

system vlan 333 // Určení systémové VLAN

state enabled // Stav ve vSphere - povolen

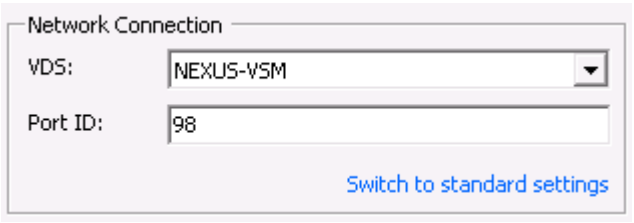
[7] CIR (Committed Information Rate) je garantovaná minimální průchodnost sítě

Po nastavení QoS na 100 Kbits/sec na L3-Vlan port-profile se propustnost rapidně snížila, to ukazuje obrázek 5.7. Docílil jsem tedy žádaného omezení. Limitování pomocí QoS je nastaveno pro vstupní i výstupní provoz port-profile.

```
------------------------------------------------------------
Client connecting to 10.1.1.14, TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[  3] local 10.1.1.12 port 49432 connected with 10.1.1.14 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-31.9 sec   384 KBytes  98.5 Kbits/sec
```

Obrázek 5.7 - Iperf výsledky testu pro nastavení QoS

Poté jsem mohl přistoupit k dalšímu testu a tím byla změna konfigurace virtuálního PC 1 na jiný port přepínače NEXUS 1000v v rámci stejného port-profile L3-Vlan. Po změně zůstalo nastavení QoS zachováno. Port virtuálního PC se mění v nastavení virtuálního PC [22]. Rozhraní pro nastavení portu pro přepínač NEXUS je zobrazeno na obrázku 5.8.



Obrázek 5.8 - Nastavení portu virtuálního PC

Dále jsem ověřoval, zda zůstane nastavení stejné při migraci na jiného ESXi hostitele. Migroval jsem tedy virtuální PC1 na druhý ESXi server a opět jsem provedl test programem Iperf. Číslo portu zůstalo zachováno, tedy virtuální PC1 je ve stejném port-profile. Výsledky testu o tom vypovídaly, QoS pravidla se aplikovala i po migraci. Při změně portu na druhém ESXi hostiteli se pravidla zachovala také. To dokazuje obrázek 5.9.

```
------------------------------------------------------------
Client connecting to 10.1.1.14, TCP port 5001
TCP window size: 64.0 KByte (default)
------------------------------------------------------------
[  3] local 10.1.1.12 port 49531 connected with 10.1.1.14 port 5001
[ ID] Interval       Transfer     Bandwidth
[  3]  0.0-29.7 sec   384 KBytes   106 Kbits/sec
```

Obrázek 5.9 - Iperf výsledky testů propustnosti po migrování virtuálního PC

Dále jsem testoval nastavení QOS přímo na „interface vethernet 2“, který odpovídá portu připojenému k virtuálnímu PC 1. Odebral jsem tedy příkaz pro nastavení QoS na port-profile L3-Vlan, poté jsem ověřil, zda je propustnost opět maximální a nastavil jsem QoS na „interface vethernet 2“. Konfigurace QoS na „interface Vethernet“ vypadala na přepínači NEXUS takto:

interface Vethernet3 *// Jedná se o interface Vethernet*

service-policy type qos input class2 *// Aplikování QoS pravidla na příchozí provoz*

service-policy type qos output class2 *// Aplikování QoS pravidla na odchozí provoz*

description PC1, Network Adapter 1 *// Popis portu*

VMware dvport 97 dvswitch uuid "03 54 20 50 55 86 e5 fb-b0 16 e9 07 50 d8 06 79" // Identifikační čílo portu

VMware vm mac 0050.56A7.5281 *// MAC adresu portu*

Otestoval jsem opět propustnost pomocí programu Iperf. Šířka pásma byla opět kolem 100 Kbits/sec, přesněji 97,3 Kbits/sec. Zkusil jsem migraci virtuálního PC1 na ESXi server 2 a taky změnu portu přepínače NEXUS. Výsledek byl stejný, nastavení omezení zůstalo zachováno. Dá se tedy říct, že nastavení limitování rychlosti na určitém „interface“ přepínače NEXUS 1000v, na kterém je připojeno virtuální PC, je funkční přes celou virtuální infrasktrukturu. Nicméně po změně port-profile na L3-Vlan2 a poté zpětném nastavení na port-profile L3-Vlan se nastavení neudrželo, i když bylo virtuální PC 1 nastaveno zpět na „interface Vethernet 3“. Propustnost po testu programem Iperf byla maximální. Lze tedy říci, že nastavení limitování přímo na „interface“ se zachovává pouze s nastavením stejného port-profile, zatímco nastavení omezení na port-profile se zachová i při změně port-profile.

Cisco NEXUS je výkonný přepínač s širokým nastavením, jaké firma Cisco nabízí ve všech svých přepínačích a směrovačích. Ukázalo se, že i po migraci virtuálních PC zůstává nastavení pravidel na přepínači NEXUS pro určité porty v daném port-profile zachováno, i po přemístění na jiného ESXi hostitele. Zachování nastavení jsem ověřil ve všech případech pomocí programu Iperf v režimu TCP. Propustnost se rovnala vždy aplikaci pravidla, které bylo nastaveno na daném port-profile.

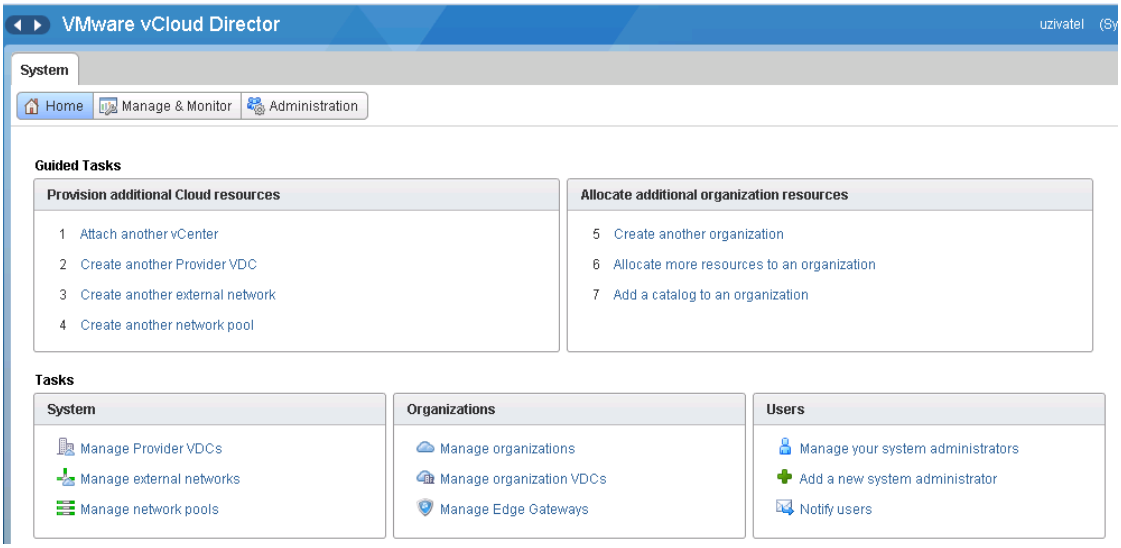
V konečném důsledku lze říci, že požadavky na síťovou infrastrukturu se zohledněním mobility virtuálních PC nejsou náročné. Sám jsem tento test realizoval v prostředí jediného přepínače a dvou ESXi serverů, které musí být kompatibilní s VMware softwarem. Poté stačí nainstalovat zkušební verze ESXi serveru, vCenter a následně zkušební verzi přepínače Cisco NEXUS 1000v.

5.3 vCloud director

Pro srovnání cloud systémů jsem si zkusil nainstalovat svůj vlastní privátní vCloud také od společnosti VMware. Nutnost pro fungování vCloud je již nainstalovaný vCenter server na ESXi hostiteli. Dále je nutné mít nainstalovaný produkt vCloud Networking and Security. Instalace vCloud director probíhá přes vSphere klienta instalací takzvaného OVF souboru.

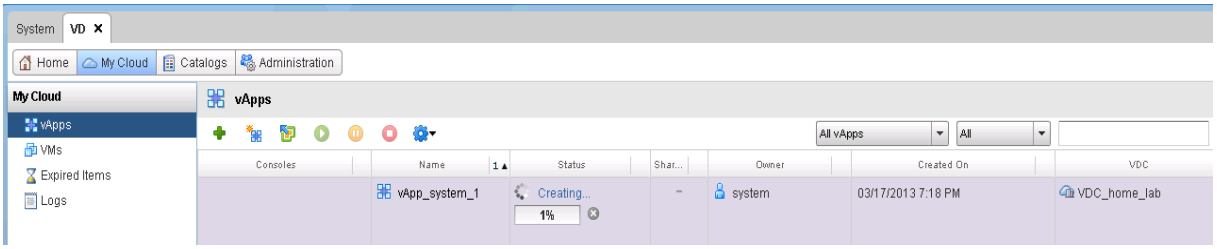
Základní konfiguraci přes webové rozhraní zobrazuje obrázek 5.10. Počáteční konfigurace vCloud Director a vCloud Networking and Security probíhá přes vShpere klienta. Na vCenter serveru je nutné mít vytvořen cluster a rezervované zdroje (resource pool). Resource pool slouží k rezervaci výkonu ESXi serveru pro virtuální PC, které jsem pod tímto resource pool ve vSphere přiřazené. Také je nutné mít povolení služby jako je High Availibilty (HA) a Distributed Resource Scheduler (DRS). Poté je teprve možné přistoupit k základní konfiguraci. Při konfiguraci se vytváří vCloud centrum, dochází ke konfiguraci EDGE gateway a dojde také k vytvoření podsítě pro virtuální PC, které jsou vytvořeny klienty vCloudu. EDGE gateway je bránou pro virtuální PC, které jsou připojeny pro připravené podsítě. V neposlední řadě je nutné ještě překonfigurovat ESXi hostitele do údržbového módu, pro spárování s vCloud director [23].

V pokročilejším nastavení se vytváří uživatelé vCloud director a tito uživatelé si mohou vytvářet jednotlivé virtuální PC a jednotlivé virtuální aplikace. Toto lze vidět na obrázku 5.11, kde právě dochází k vytvoření virtuální aplikace.



Obrázek 5.10 - vCloud director- základní konfigurace privátního cloud

Přes webové rozhraní je možné spravovat také virtuální PC. Virtuální PC, vytvořené přes webové rozhraní, jsou zobrazovány ve vSphere klientovi v takzvaném resource pool. Tyto virtuální PC lze přes vSphere klienta také libovolně editovat, přesouvat atd. Virtuální PC, které nejsou vytvořené v vCenter serveru pod resource pool, nejdou vidět přes webového klienta vCloud.



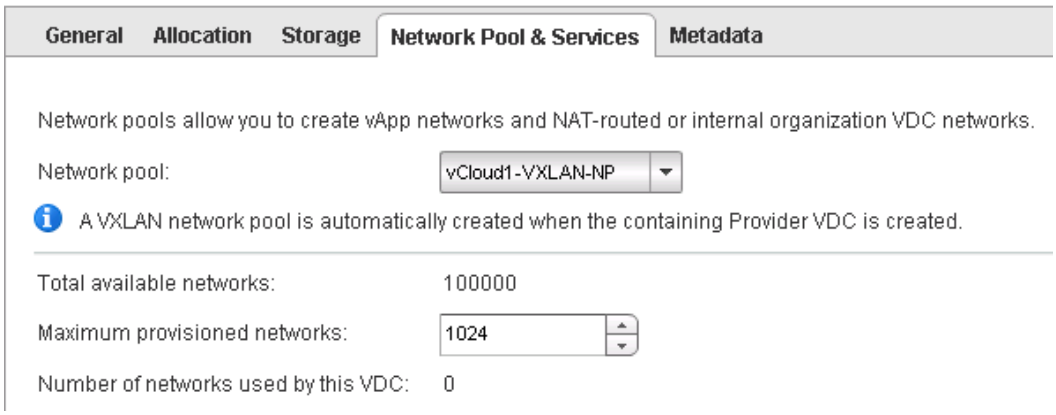
Obrázek 5.11 - Vytvoření virtuální aplikace v vCloud

Práce s webovým klientem je celkem jednouchá a uživatelsky nenáročná. Kromě počátečního nastavení, které je poměrně náročné na pochopení pojmů, je práce s vCloud vhodná pro IT administrátory. Nejvíce času mi zabrala konfigurace síťové části u vCloud director, protože je docela komplexní – lze zde vytvořit oddělené virtuální sítě od sítí na jednotlivých ESXi hostitelích. Také je možné pomocí takzvané EDGE Gateway vytvořit propojení sítí korporátního datacentra nebo i vlastní síť s přístupem k Internetu. EDGE Gateway poté funguje jako směrovač s PAT.

Klíčovým nastavením ve vCloudu je nastavení práv a úloh, které mohou jednotliví uživatelé vytvářet. Odvíjí se od toho také, jestli mohou jednotliví uživatelé vytvářet virtuální PC a aplikace. Pro jednodušší funkčnost celého vCloud je dobré přednastavit šablony virtuální počítače všech systémů a tak zamezit zbytečnému využívání výkonu pro virtuální PC se systémy, které to nepotřebují.

Oproti vSphere klientovi lze nastavit a vytvořit ve vCloud director VXLAN, jejímž popisem jsem se zabýval v kapitole 3.3.4. VXLAN se vytvoří implicitně s vytvořením každého vCloud, pouze pro její plnou funkčnost je nutné před-konfigurovat produkt vCloud Networking and Security. Ve vCenter je nutné vytvořit DvSwitch a do něho připojit alespoň jednu síťovou kartu od každého ESXi hostitele. Až poté lze aktivovat VXLAN, která je implicitně před-vytvořená ve vCloud.

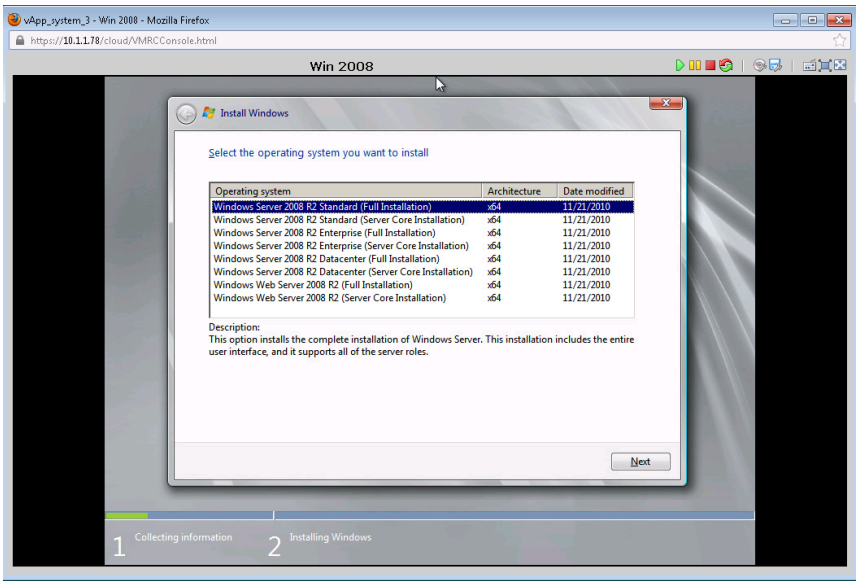
Na obrázku 5.12 je vidět konfigurace VXLAN ve vCloud. Toto nastavení je výhodou v rozsáhlých sítí, kde je potřeba opravdu mnoho VLAN.



Obrázek 5.12 - VXLAN ve vCloud

vCloud 5.1 běží pod různými prohlížeči, já osobně jsem vyzkoušel kompatibilitu Internet Explorer 10 a Firefox 19. V obou prohlížečích probíhala práce s cloud bez problémů. Na obrázku 5.13 je zobrazeno spuštění virtuálního PC, a také vzhled jaký má vCloud v prohlížeči. Plynulost v obou prohlížečích byla dobrá, odezvy v pořádku. Práce pomocí plnohodnotného vSphere klienta je o něco rychlejší, jde to poznat u odezev myší. Připojovat obraz disků lze taky jako z vSphere klienta. Z pohledu klienta, může práce s vCloud v prohlížeči, až na malé výhrady, nahradit práci přes vSphere klienta.

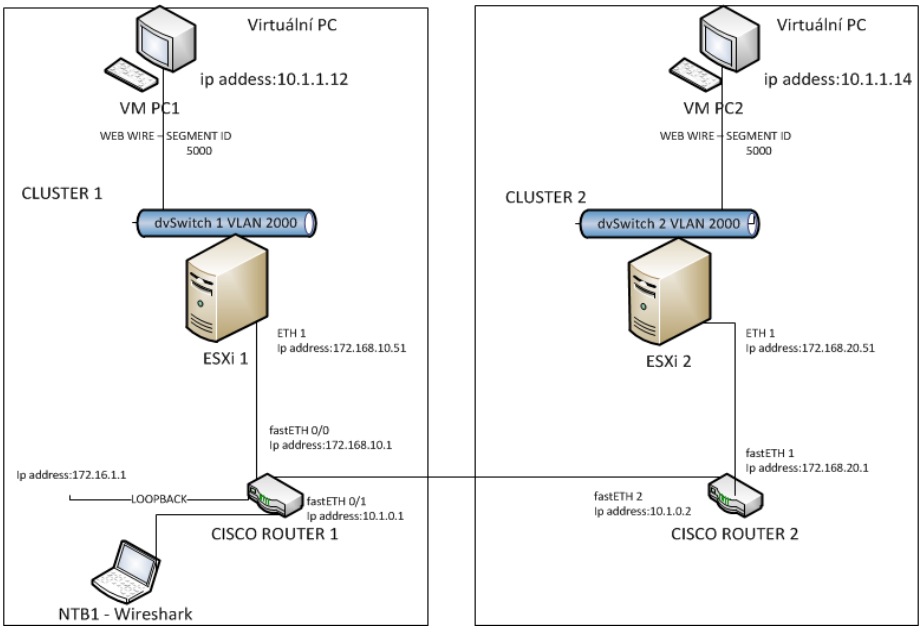
vCloud director je tedy velice silným nástrojem pro provoz Cloud služeb, rozdělení práv a výkonu ESXi hostitelů. Kdybych měl srovnat IBM private Cloud a VMware vCloud tak mohu říci, že se jedná o dvě stejná řešení, s tím rozdílem, že IBM Cloud je dodáván s přídavným softwarem pro snadnější správu cloud systému. Tento produkt se jmenuje IBM Service Delivery Manager.



Obrázek 5.13 - vCloud - instalace Windows 2008 v prohlížeči

5.4 Ověření funkčnosti VXLAN přes L3

V této kapitole bych se chtěl zaměřit na ověření průchodu paketů VXLAN přes směrovače Cisco po L3. Topologie pro tento test je zobrazena na obrázku 5.14. Pro tento test jsem si zapůjčil dva Cisco směrovače CISCO881-K9. Zajímalo mě, jestli se nějak liší pakety při komunikaci dvou PC ve virtualizovaném prostředí při připojení do VXLAN.



Obrázek 5.14 - Schéma zapojení sítě při testu VXLAN

Nutností pro tento test byl nainstalovaný produkt vCloud Networking and Security. V mém prostředí, které se skládalo ze dvou ESXi serverů, jsem vytvořil dva clustery a do každého clusteru umístil jeden ESXi server. Poté jsem nainstaloval produkt vCloud Networking and Security pomocí souboru OVF. Dále bylo nutné produkt vCloud Networking and Security nakonfigurovat. Prvotní nastavení produktu probíhá přes vSphere koznoli. V konzoli jsem nastavil IP adresu pro tento produkt. Dále už probíhá konfigurace přes webové rozhraní. vCloud Networking and Security je interpretován v celé infrastruktuře jako virtuální PC.

Ve vCenter server je nutné vytvořit dva dvSwitch. Jeden jsem pojmenoval jako dvSwitch1 a druhý jako dvSwitch2. Do obou dvSwitch jsem přidal jeden ESXi server, pro spojení clusterů s celou infrastrukturou. Nastavení VLAN na clusterech ilustruje obrázek 5.15. Na cluster1 a cluster 2 jsem nastavil VLAN 2000.

Hosts & Clusters	Status	Vmknic IP Addresses	Distributed Switch	VLAN
Cluster1	Ready	DHCP	dvSwitch1	2000
10.1.1.231	Ready	vmk1:172.168.10.51		
Cluster2	Ready	DHCP	dvSwitch2	2000
10.1.1.245	Ready	vmk1:172.168.20.51		

Obrázek 5.15 - Nastavení VLAN na clusterech

Pro management rozhraní obou ESXi serverů jsem nastavil pevné IP adresy na obou dvSwitch:

- na dvSwitch1 IP adresu 172.168.10.1 a masku 255.255.255.0

- na dvSwitch2 IP adresu 172.168.20.1 a masku 255.255.255.0

Poté jsem si vytvořil dvě port-group v rámci dvSwtich 1 a 2 – jednu pro datovou komunikaci s názvem DATA a druhou pro komunikace s internetem s názvem WEB, což je vidět na obrázku 5.16.

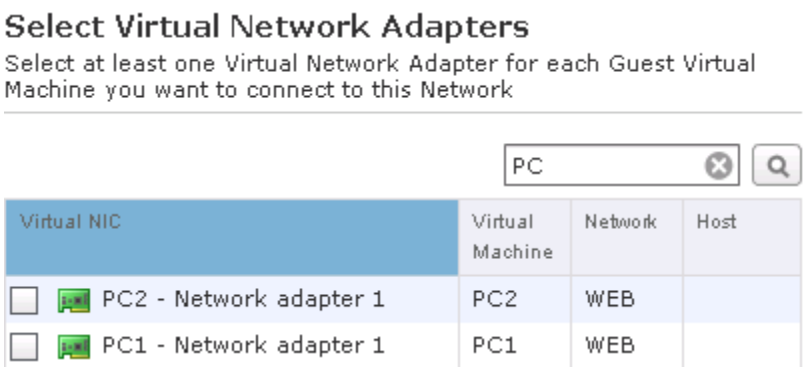
Name	Status	Segment ID	Multicast IP Address
DATA	OK	5001	225.1.1.2
WEB	OK	5000	225.1.1.1

Obrázek 5.16 - Nastavení virtuální port-group pro dvSwitch 1 a 2

Na obrázku 5.16 vpravo je také zobrazena multicast skupina pro jednotlivé port-group DATA a WEB. Jde o to, že komunikace mezi ESXi servery bude pro každou port-group enkapsulována do multicast paketu s cílovou multicast skupinou – podle toho o jakou port-group půjde. Také dojde k mapováníVXLAN Network Identifier (VNI) jednotlivých port-gorup na multicast skupiny. VNI je zobrazeno vlevo vedle sloupce „Multicast IP Address“ na obrázku 5.16.

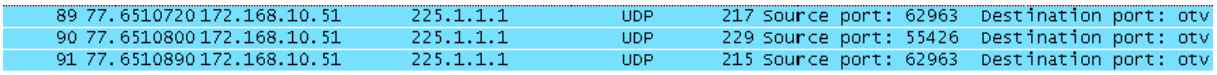
Tímto konfigurace na straně vSphere skončila a bylo nutné nastavit směrovače Cisco. Na směrovači R1 jsem nastavil IP adresu 172.168.10.1 a masku 255.255.255.0. Na směrovači R2 jsem nastavil IP adresu 172.168.20.1 a masku 255.255.255.0. Poté jsem směrovače propojil podle obrázku 5.14. . Konfigurace obou Cisco přepínačů je zobrazena v příloze A.

Testovaným PC1 a PC2 jsem nastavil port-group jménen WEB u obou dvSwich. To lze udělat dvěma způsoby. První způsob je nastavit vlákno WEB přímo na virtuálním PC přes vSphere a druhý způsob je nastavit vlákno WEB přímo přes webové rozhraní produktu vCloud Networking and Security. Rozhraní pro přidání síťových karet virtuálních PC1 a PC2 ukazuje obrázek 5.17.



Obrázek 5.17 - Přidání virtuálních adaptérů PC1 a PC2

Při tom jsem ještě testoval nastavení na směrovačích Cisco a vyzkoušel jsem ping z PC1 na PC2, který úspěšně prošel. Ještě mě zajímalo, jak vypadá ICMP paket, který přes síť prochází. Připojil jsem si NTB1 do směrovače R1 do portu, na kterém je nastavené kopírování provozu z ETH2 směrovače R1. Poté jsem spustil Wireshark a poslouchal jsem provoz mezi dvěma ESXi servery. Při spuštění příkazu ping na IP adresu 10.1.1.14, začne PC1 požadovat MAC adresu IP adresy 10.1.1.14. Dojde tedy k enkapsulaci ARP paketu, posílaného pro broadcast, do multicast paketu a ten se pošle na skupinu 225.1.1.1 s VXLAN hlavičkou pro VNI 5000. Cisco směrovač R1 zaregistruje jako zdroj ESXi server 1 s IP adresou 172.168.10.51 pro skupinu 225.1.1.1 jako rendezvous point[8]. ESXi server 2 dostane multicast paket pro skupinu 225.1.1.1 asociovanou s VNI 5000. Po dekapsulaci paketu dojde k odeslání paketu příjemci, tedy PC2, který je přihlášen do virtuálního vlákna s VNI 5000. Poté dojde k uložení MAC adresy PC2 do VXLAN mapovací tabulky. Směrovač Cisco R2 se poté napojí na skupinu 225.1.1.1 ESXi serveru 1. ESXi server 2 enkapsuluje odpověď jako unicast paket a pošle ji ESXi serveru 1 přes směrovače R1 a R2. Výřez z programu Wireshark na obrázku 5.18. ukazuje multicast paket, ve kterém je enkapsulovaný ARP paket pro skupinu 225.1.1.1. Pokud bych v programu Wireshark dekódoval komunikaci jako VXLAN, došlo by k zobrazení ARP dotazu poslanou pro broadcast. Dekódovanou hlavičku VXLAN v programu Wireshark lze vidět na obrázku 5.19, kde už není vidět multicast komunikace, ale ICMP dotaz.

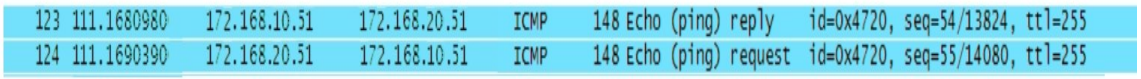


Obrázek 5.18 - Wireshark - ARP pakek

I když byl ARP dotaz vyslán z PC1 (10.1.1.12), tak je ve Wiresharku vidět, že se ptá IP adresa 172.168.10.51, což je vlastně ESXi server 1. Enkapsulace totiž začíná při zpracování paketu ESXi serverem.

Poté už bude ping komunikace probíhat mezi ESXi servery přes unicast. Při komunikaci jednotlivých PC dojde k enkapsulaci paketu do VXLAN hlavičky s VNI 5000. Unicast komunikace je vidět naobrázku 5.19, na kterém je zobrazen ICMP paket, tedy příkaz ping z PC1 na PC2 na prvním řádku a na druhém řádku odpověď od PC2 k PC1. Komunikace probíhá enkapsulována do VXLAN hlavičky a posílají si jí dva ESXi servery mezi sebou, proto jsou zde zmíněny IP adresy 172.168.10.51 a 172.168.20.51.

[8] Rendezvous Point (RP) je nastaven na směrovači, který funguje v multicast síťové doméně jako root pro multicast komunikaci



Obrázek 5.19 - Wireshark - Ping příkaz, dekodován jako VXLAN

Zkoušel jsem spustit program Wireshark na jednom z virtuálních PC. Výsledek byl takový, že jednotlivé požadavky a odpovědi tam byly zobrazeny, jako kdyby byly počítače spojeny jedním přepínačem. Z této komunikace už nejde poznat, že došlo k enkapsulaci a dekapsulaci paketu v rámci VXLAN. Dotaz byl zobrazen z PC1 a IP adresy 10.1.1.12 na PC 2 s IP adresou 10.1.1.14. Virtuální počítače komunikaci vidí, jako kdyby byla poslána po L2 síti

Komunikace mezi jednotlivými ESXi servery je tedy enkapsulována do VXLAN paketu a jak jsem viděl v programu Wireshark, tuto komunikaci lze rozlišit při srovnání s komunikací obyčejné VLAN.

6 Závěr

Virtualizace se v současnosti hodně rozšiřuje, hlavně z důvodu nahrazení stávající infrastruktury a optimalizace nákladů. V dnešní době je konkurence virtualizačních softwarů velká. Mezi nejhlavnější firmy poskytující virtulazaci patří Microsoft, IBM a VMware. Virtualizace je hlavně vhodná pro firmy, jejichž produktivita je závislá na provozu serverů bez možnosti nějakého výpadku. Toto lze docílit s tím, že bude postavena na více ESXi serverech. Tímto se zajistí 100% záloha proti výpadku při provozu, například při výpadku jednoho ESXi serveru. V této situace beru v úvahu, že všechny servery a aktivní prvky jsou připojeny na záložním zdroji. Když se podívám na tento příklad z druhé strany, při výpadku reálného serveru by došlo ke ztrátám produkce na dobu, po kterou by trvala oprava daného hardware, případně software serveru. Výhody virtualizace nejsou jen v záloze provozu běžících serverů, ale také při nedostatku VLAN v sítích. Lze zde využít takzvanou VXLAN, která mnohonásobně rozšíří počet VLAN v infrastruktuře.

Věřím, že tato práce pomůže dalším IT pracovníkům rozhodnout se, kterým směrem při virtualizaci jít a co všechno lze od virtualizace čekat. Jak se v práci ukázalo, virtualizace je dnes na velmi vysoké úrovni a také testy dokladují, že například virtuliazce od VMware má velice široké spektrum nastavení. Rozbory řešení virtualizace jednotlivých firem jsem se snažil poukázat na výhody a nevýhody. Jak se v práci ukázalo, prostředí virtualizace od VMware je velice uživatelsky přístupné, nicméně nabízí také široké spektrum nastavení pro danou infrastrukturu. V neposlední řadě jsem se zaměřil na možnosti rozšíření virtualizace od VMware a to pomocí takzvaných pluginů, které jdou pomocí vSphere klienta jednoduše nainstalovat. Také jsem rozkryl nastavení a možnosti VXLAN, kdy lze pomocí zapouzdření L2 sítě do L3 paketů rozprostřít VXLAN mezi různými sítěmi. Ověřil jsem tvrzení, že VXLAN komunikace mezi dvěma ESXi servery probíhá po L3. Také jsem prozkoumal možnosti produktu vCloud od VMware a srovnal používání webového prohlížeče pro práci s virtuálními PC oproti používání vSphere klienta. U přepínače Cisco NEXUS 1000v jsem otestoval zachování nastavení na portu pomocí port-profile, i při migraci na jiný ESXi server. Pokud ale dojde k nastavení omezení přímo na „interface“ konkrétního portu přepínače NEXUS, při změně port-profile nezůstane nastavení zachováno. Proto Cisco doporučuje nastavení portů konfigurovat pomocí port-profile.

Naplnění hlavního cíle, a to prozkoumání možností a vlastností virtuální infrastruktury, bylo dosaženo. Na základě této práce jsem úspěšně zvirtualizoval servery v naší firmě, které musí být v provozu 24 hodin denně. Během tří měsíčního provozu jsem zatím nezaznamenal jejich výpadek.

Celkově tak práce podává informace, jak využít nový fenomén cloud computing ke svému užitku a získat z něj maximální možný přínos.

Použitá literatura

[1] Salesforce. *What is Cloud Computing* [online]. c2013 [cit 2013-01-30]. Salesforce.com. Dostupné z WWW: <http://www.salesforce.com/cloudcomputing/>.

[2] Wikipedia. *Cloud Computing* [online]. 23. dubna 2013 [cit 2013-02-02]. Wikipedia.org. Dostupný z WWW: <http://upload.wikimedia.org/wikipedia/commons/thumb/b/b5/Cloud_computing.svg/400px-Cloud_computing.svg.png>.

[3] IBM. *Define your cloud* [online]. c2013 [cit 2013-02-3]. Ibm.com. Dostupné z WWW: <http://www.ibm.com/systems/cloud>.

[4] VMware Inc. *Řešení cloud computing* [online]. c2012 [cit 2013-02-12]. VMware.com. Dostupné z WWW: <http://www.VMware.com/cz/cloud-computing.html>.

[5] Microsoft. *Cloud Power* [online]. c2013 [cit 2013-02-10]. Microsoft.com. Dostupné z WWW: <http://www.microsoft.com/cze/cloud/>.

[6] IBM. *IBM Service Delivery Manager* [online]. c2013 [cit 2013-02-15]. Ibm.com. Dostupné z WWW: <http://www-01.ibm.com/software/tivoli/products/service-delivery-manager/>.

[7] IBM. *IBM SmartCloud Enterprise* [online]. c2013 [cit 2013-02-14]. 395.ibm.com. Dostupné z WWW: <http://www-935.ibm.com/services/cz/cs/cloud-enterprise/>.

[8] VMware. *Private cloud computing* [online]. c2013 [cit 2013-02-16]. VMware.com. Dostupné z WWW: <http://www.VMware.com/solutions/cloud-computing/private-cloud/index.html>.

[9] O2. *O2 Cloud* [online]. c2013 [cit 2013-02-16]. O2.cz. Dostupné z WWW: <http://www.o2.cz/corporate/269811-cloudova_reseni/o2_cloud.html>.

[10] O2. *O2 Cloud pomáhá nově také inkubátoru ČVUT* [online]. 15. května 2012 [cit 2013-03-16]. Mobile.o2.cz/corporate. Dostupný z WWW: <http://mobile.o2.cz/corporate/200519-tiskove_zpravy/285311-O2_Cloud_pomaha_nove_take_inkubatoru_CVUT.html>.

[11] Microsotf System Center 2012. *System Center 2012* [online]. c2013 [cit 2013-02-16]. Microsoft.com. Dostupné z WWW: <http://www.microsoft.com/cs-cz/server-cloud/system-center/default.aspx>.

[12] Pavel Řepa – IT management (CZ). *První pohled na System Center Configuration Manager 2012* [online]. 21.12.2011 [cit 2013-02-17]. Pavelrepa.wordpress.com. Dostupné z WWW: <http://pavelrepa.wordpress.com/tag/security/>.

[13] Lowe, Scott. *Mistrovství ve VMware vSphere 5 Kompletní průvodce profesionální virtualizací*. COMPUTER PRESS, 6. Února 2013. ISBN 9788025137741.

[14] VMware. *VMware vSphere 5.1 Documentation Center* [online]. c1998 [cit 2013-02-14]. Pubs.VMware.com. Dostupné z WWW: <http://pubs.VMware.com/vsphere-51/index.jsp>.

[15] KB VMware. *Sample configuration EtherChannel* [online]. c2013 [cit 2013-02-22]. Kb.VMware.com. Dostupné z WWW: <http://kb.VMware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1004048>.

[16] Maille, Eric a Mennecier, René-Francois. *VMware vSphere 5® Building a Virtual Datacenter. 1*. Vydání.VMware Press, 20. srpna 2012. ISBN 0321832213.

[17] Cisco Systems, Inc. *Cisco Nexus 1000V Series Switches* [online]. c2013 [cit 2013-03-01]. Cisco.com. Dostupné z WWW: <*http://www.cisco.com/en/US/products/ps9902/index.html*>.

[18] Lowe, Scott. *Mastering VMware vSphere 5. 1*. Vydání. Sybex, 29. září 2011. ISBN 0470890800.

[19] VMware, Inc. *Performance Best Practices for VMware vSphere® 5.1*: VMware ESXi™ 5.1, vCenter™ Server 5.1 [online]. c2012 [cit 2013-03-01]. VMware.com. Dostupný z WWW: <http://www.vmware.com/pdf/Perf_Best_Practices_vSphere5.1.pdf>.

[20] IProsperita. *VMware vCenterOperations* [online]. c2012 [cit 2013-03]. IProsperita.cz. Dostupné z WWW:

<http://www.IProsperita.cz/it-a-komunikace/
110--VMware-prichazi-s-vcenter-operations-novym-operacnim-modelem-pro-prostredi-Cloudu>.

[21] Router Jockey. *QinQ: IEEE 802.1Q Tunneling* [online]. c2013 [cit 2013-02-22]. Routerjockey.com. Dostupné z WWW: <http://routerjockey.com/2012/04/19/qinq-ieee-802-1q-tunneling/>.

[22] Cisco support community. *Nexus 1000v: QoS Overview and Traffic Classification Configuration* [online]. c1992 [cit 2013-03-05]. Supportforums.cisco.com. Dostupné z WWW: <https://supportforums.cisco.com/docs/DOC-27151>.

[23] Oldany Group. *VMware Cloud Director* [online]. c2013 [cit 2013-03-08]. Oldanygroup.cz. Dostupné z WWW: *<http://www.oldanygroup.cz/VMware-vcloud-director-270/>*.

[24] WAHLNETWORK. *New 5.1 Distributed Switch* [online]. c2013 [cit 2013-03-25]. Wahlnetwork.com. Dostupné z WWW: http://wahlnetwork.com/2012/08/27/new-5-1-distributed-switch-features-part-3-port-mirror-and-netflow-enhancements/

[25] Eric Sloof – NTPRO.NL. *vCenter Operations* [online]. c2013 [cit 2013-03-25]. Ntpro.nl. Dostupný z WWW: <http://www.ntpro.nl/blog/uploads/vCops-1.png>.

[26] BUREAUCLOUD. *vCloud Networking and Security* [online]. c2011 [cit 2013-03-25]. Support.bureaucloud.com. Dostupný z WWW: <https://support.bureaucloud.com/support/index.php?pg=file&from=2&id=41>.

[27] Microsoft Corporation. *Cisco NEXUS 1000v* [online]. c2013 [cit 2013-03-25]. Virtualizationadmin.com. Dostupný z WWW: <http://blogs.virtualizationadmin.com/davis/wp-content/blogs/59/files/2009/05/cisco%20nexus%201000v%20architecture.jpg>.

[28] Microsoft Corporation. *Microsft vs VMware* [online]. 15. února 2013 [cit 2013-03-25]. Mstv.cz. Dostupný z WWW: <http://www.mstv.cz>.

[29] IBM. *IBM SmartCloud Services trial* [online]. c2013 [cit 2013-03-25]. Ibm.com/developerworks. Dostupný z WWW: <http://www.ibm.com/developerworks/cloud/cloudtrial.html>.

Seznám obrázků

Seznam tabulek

Přílohy

Seznam příloh

Příloha A: Konfigurace Cisco směrovačů

Konfigurace směrovače R1 vypadala takto:

```
hostname R1
!
ip multicast-routing
!
interface Loopback0
description PIM RP
ip address 172.16.1.1 255.255.255.255
ip pim sparse-mode
!
interface FastEthernet0/0
ip address 172.168.10.1 255.255.255.0
no ip proxy-arp
ip pim sparse-mode
duplex auto
speed auto
!
interface FastEthernet0/1
ip address 10.1.0.1 255.255.0.0
ip pim sparse-mode
duplex auto
speed auto
!
router ospf 1
log-adjacency-changes
passive-interface FastEthernet0/0
```

network 10.1.0.0 0. 0.255.255 area 0

network 172.16.1.1 0.0.0.0 area 0

network 172.168.0.0 0.0.255.255 area 0

!

ip pim rp-address 172.16.1.1

!

Konfigurace směrovače R2 vypadala takto:

hostname R2

!

ip multicast-routing

!

interface FastEthernet0/0

ip address 172.168.20.1 255.255.255.0

no ip proxy-arp

ip pim sparse-mode

duplex auto

speed auto

!

interface FastEthernet0/1

ip address 10.1.0.2 255.255.0.0

ip pim sparse-mode

duplex auto

speed auto

!

router ospf 1

log-adjacency-changes

passive-interface FastEthernet0/0

network 10.1.0.0 0. 0.255.255 area 0

network 172.16.1.1 0.0.0.0 area 0

network 172.168.0.0 0.0.255.255 area 0

!

ip pim rp-address 172.16.1.1

!

Příloha B: Adresářová struktura přiloženého CD

/Diplomová práce	Diplomová práce v dokumentu pdf
/Konfigurace ESXi serverů podle kapitoly 5.1	Záloha konfigurace ESXi serverů a Mikrotiku
/Konfigurace ESXi serverů podle kapitoly 5.2	Záloha konfigurace ESXi serverů a přepínače NEXUS 1000v
/Konfigurace ESXi serverů podle kapitoly 5.4	Záloha konfigurace ESXi serverů